

LATEST
EDITION



Comparing privacy laws: GDPR v. CCPA



December 2019

OneTrust
DataGuidance™
REGULATORY RESEARCH SOFTWARE

 **FUTURE OF
PRIVACY
FORUM**

About the authors

OneTrust DataGuidance provides a suite of privacy solutions designed to help organisations monitor regulatory developments, mitigate risk and achieve global compliance.

The OneTrust DataGuidance platform includes focused guidance around core topics (i.e. GDPR, data transfers, breach notification, among others), Cross-Border Charts which allow you to compare regulations across multiple jurisdictions at a glance, a daily customised news service and expert analysis.

These tools, along with our in-house analyst service to help with your specific research questions, provide a cost-effective and efficient solution to design and support your privacy programme.

Future of Privacy Forum is a nonprofit organization that serves as a catalyst for privacy leadership and scholarship, advancing principled data practices in support of emerging technologies. FPF brings together industry, academics, consumer advocates, and other thought leaders to explore the challenges posed by technological innovation and develop privacy protections, ethical norms, and workable business practices.

Contributors

OneTrust DataGuidance: Alice Marini, Alexis Kateifides, Nikolaos Papageorgiou, Joel Bates, Victoria Ashcroft

Future of Privacy Forum: Gabriela Zanfiri-Fortuna, Michelle Bae, Stacey Gray, Jeremy Greenberg, Gargi Sen

Image production credits:

Cover/p.3/p.43: Bulgac / Signature collection / istockphoto.com, cnythzl / Signature collection / istockphoto.com
Scale key p6-39: enisaksoy / Signature collection / istockphoto.com
Icon p.25-37: AlexeyBlogoodf / Essentials collection / istockphoto.com

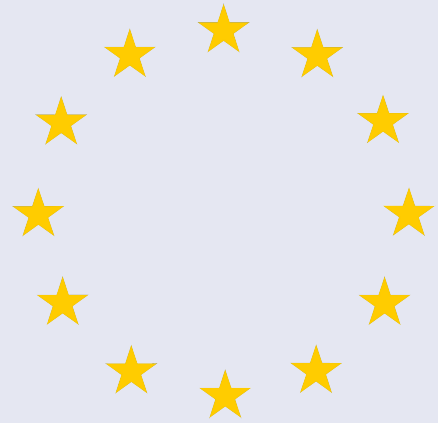
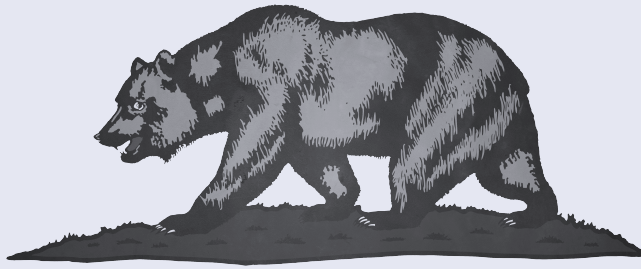


Table of contents

Introduction	5
1. Scope	
1.1. Personal scope	7
1.2. Territorial scope	8
1.3. Material scope	9
2. Key definitions	
2.1. Personal data (personal information)	13
2.2. Pseudonymisation	16
2.3. Controllers and processors (businesses and service providers)	17
2.4. Children	19
2.5. Research	21
3. Legal basis	25
4. Rights	
4.1. Right to erasure (right to deletion)	26
4.2. Right to be informed	28
4.3. Right to object (right to opt-out)	30
4.4. Right of access	31
4.5. Right not be subject to discrimination for the exercise of rights	33
4.6. Right to data portability	34
5. Enforcement	
5.1. Monetary penalties	37
5.2. Supervisory authority	38
5.3. Civil remedies for individuals	39
Index: CCPA provisions	41



Introduction

The General Data Protection Regulation (Regulation (EU) 2016/679) ("GDPR") and the California Consumer Privacy Act of 2018 ("CCPA") (SB-1121 as amended at the time of this publication) both aim to guarantee strong protection for individuals regarding their personal data and apply to businesses that collect, use, or share personal data, whether the information was obtained online or offline.

The GDPR, which went into effect on 25 May 2018, is one of the most comprehensive data protection laws in the world to date. Absent a comprehensive federal privacy law in the U.S., the CCPA is considered to be one of the most significant legislative privacy developments in the country. Like the GDPR, the CCPA's impact is expected to be global, given California's status as the fifth largest global economy. The CCPA will take effect on 1 January 2020, but certain provisions under the CCPA require organizations to provide consumers with information regarding the preceding 12-month period, and therefore activities to comply with the CCPA may well be necessary sooner than the effective date.

As highlighted by this Guide, the two laws bear similarity in relation to their definition of certain terminology; the establishment of additional protections for individuals under 16 years of age; and the inclusion of rights to access and delete personal information.

However, the CCPA differs from the GDPR in some significant ways, particularly with regard to the scope of application; the nature and extent of collection limitations; and rules concerning accountability. Regarding the latter for example, the GDPR provides for obligations in relation to the appointment of Data Protection Officers, the maintenance of a register of processing activities, and the need for Data Protection Impact Assessments in specified circumstances. Conversely, the CCPA does not specifically focus on accountability-related obligations, even though such provisions exist, such as the obligation for companies to train their staff that deal with requests from consumers.

It is also noteworthy that the core legal framework of the CCPA is quite different from the GDPR. A fundamental principle of the GDPR is the requirement to have a "legal basis" for all processing of personal data. That is not the case for the CCPA.

In addition, the CCPA excludes from its scope the processing of some categories of personal information altogether, such as medical data covered by other U.S. legal frameworks, including processing of personal information for clinical trials, and personal information processed by credit reporting agencies. Moreover, the CCPA focuses on transparency obligations and on provisions that limit selling of personal information, requiring a "Do Not Sell My Personal Information" link to be included by businesses on their homepage. In addition, the CCPA includes specific provisions in relation to data transferred as a consequence of mergers and acquisitions.

A series of bills, signed by the California Governor on 11 October 2019, amended the CCPA to exempt from its application certain categories of data and to provide different requirements for submission of consumer requests, among other things. The Guide has been updated to take into account these amendments.

Finally, the California Attorney General issued, on 10 October 2019, Proposed Regulations under the CCPA which are intended to provide practical guidance to consumers and businesses. The Proposed Regulations were open for public consultation until 6 December 2019 and, when finalised, will provide an additional layer of regulatory requirements that companies will have to comply with.


This updated Guide aims to assist organisations in understanding and comparing the relevant provisions of the GDPR and the CCPA, to ensure compliance with both laws.


Structure and overview of the Guide


This Guide provides a comparison of the two pieces of legislation on the following key provisions:


1. Scope
2. Key definitions
3. Legal basis
4. Rights
5. Enforcement

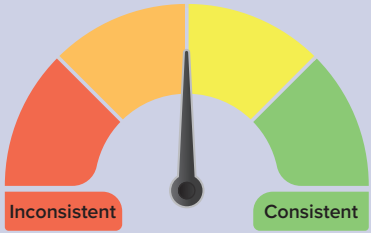
Each topic includes relevant articles and sections from the two laws, a summary of the comparison, and a detailed analysis of the similarities and differences between the GDPR and the CCPA. The degree of similarity for each section can be identified using the key below.

 **Consistent:** The GDPR and CCPA bear a high degree of similarity in the rationale, core, scope, and the application of the provision considered.

 **Fairly consistent:** The GDPR and CCPA bear a high degree of similarity in the rationale, core, and the scope of the provision considered; however, the details governing its application differ.

 **Fairly inconsistent:** The GDPR and CCPA bear several differences with regard to the scope and application of the provision considered, however the rationale and core present some similarities.

 **Inconsistent:** The GDPR and CCPA bear a high degree of difference with regard to the rationale, core, scope and application of the provisions considered.



Usage of the Guide

This Guide is general and educational in nature and is not intended to provide, and should not be relied on as a source of legal advice. The information and materials provided in the Guide may not be applicable in all (or any) situations and should not be acted upon without specific legal advice based on particular circumstances.

The analysis is based on the version of the CCPA amended by the California legislature in October 2019. Please note that the CCPA provides a mechanism for additions or changes to some provisions through rulemaking by the California Attorney General.

1. Scope



Fairly inconsistent

1.1. Personal scope

With regard to personal scope, businesses, public bodies and institutions, as well as not-for-profit organizations are subject to the GDPR, whilst only for-profit entities ("businesses") are covered under the CCPA. In addition, the CCPA sets thresholds that determine businesses covered by the law, while the GDPR does not. Both laws apply to those businesses that determine the "purposes and means of the processing" of data.

The CCPA protects "consumers" who are natural persons and who must be California residents in order to be protected, whilst the GDPR protects "data subjects," who are natural persons and does not specify residency or citizenship requirements. The CCPA provisionally excludes employees from its scope, while the GDPR fully protects employee data.

GDPR	CCPA
Articles 3, 4(1) Recitals 2, 14, 22-25	Sections 1798.140 (c), (g), 1798.145(a)(6)

Similarities

The GDPR only protects natural persons (individuals) and does not cover legal persons.

GDPR obligations primarily apply to controllers. A controller is defined by the fact that it establishes the means and purposes of the processing.

The CCPA only protects natural persons (individuals) and does not cover legal persons.

A covered business is defined by the fact that it establishes the means and purposes of the processing, though there are also other criteria to be met (see below).

Differences

Article 4(1) of the GDPR clarifies that a **data subject** is "**an identified or identifiable natural person.**" Article 3 and Recitals 2, 14, and 24 provide that a data subject may be any individual whose personal data is processed, and do not specifically require that the data subject holds EU residency or citizenship, or is located either within or outside the EU. However, there is a location-related requirement as a condition to trigger applicability when the controller does not have an establishment in the EU (see below). A data subject must be a living individual as the GDPR does not cover the processing of personal data of deceased persons.

The GDPR obligations apply to "**controllers,**" which can be natural or legal persons, irrespective of whether their activity

A "**consumer**" who has rights under the CCPA is "**a natural person who is a California resident.**" The California Code of Regulations defines a resident as "(1) every individual who is in the State for other than a temporary or transitory purpose, and (2) every individual who is domiciled in the State who is outside the State for a temporary or transitory purpose. All other individuals are nonresidents."

The CCPA obligations apply to an organization ("**business**") that:

1. is **for-profit;**

Differences (cont'd)

is for profit or not, irrespective of their size and whether they are private law or public law entities, as long as they determine the means and purposes of processing activities.

2. collects **consumers' personal information**, or on the behalf of which such information is collected;
3. **determines the purposes and means** of the processing of consumers' personal information;
4. **does business in California**; and
5. meets any of the following thresholds:
 - has **annual gross revenue in excess of \$25 million**;
 - alone or in combination, **annually buys, receives for the business's commercial purposes, sells or shares for commercial purposes the personal information of 50,000 or more consumers, households, or devices**; or
 - **derives 50% or more of its annual revenues from selling consumers' personal information**.

Several obligations also apply to "**processors**," which are entities that process personal data on behalf of controllers. For example, processors have to maintain a record of processing activities pursuant to Article 30 of the GDPR

The CCPA also applies to any entity that controls or is controlled by the business. There are no obligations directed specifically at "**service providers**," other than using the personal information solely at the direction of the business they serve. Businesses may also direct service providers to delete consumers' personal information from their records.

1.2. Territorial scope



The GDPR applies to organizations outside the EU if they offer goods or services to, or monitor the behavior of, persons within the EU. The CCPA applies to businesses that do business in California and, although not explicitly mentioned, the CCPA appears to be applicable to a business established outside of California if it collects or sells California consumers personal information while conducting business in California.

GDPR	CCPA
Articles 3, 4(1) Recitals 2, 14, 22-25	Sections 1798.140 (c), (g), 1798.145(a)(6)

Similarities

The GDPR applies to organizations that **do not have any presence in the EU**, but that **offer goods, services or monitor the behavior of persons in the EU**.

It is unclear whether the CCPA applies to a business established outside of California if it collects or sells **California consumers personal information while conducting business in California and meet one of the other quantitative thresholds**. This would depend on how "doing business in California" is interpreted and applied (see below).

Differences

Under Article 3, the GDPR applies to:

- 1. entities or organizations established in the EU:** the GDPR applies to processing by controllers and processors in the EU (entities that have an "establishment" in the EU) if processing of personal data takes place in the context of the activities of that establishment, irrespective of whether the data processing takes place in the EU or not. **"Establishment"** in the EU is interpreted broadly, which could include having a minimal presence of using a local agent or having a single representative.
- 2. entities or organizations not established in the EU:** the GDPR also applies to organisations located outside the EU (those that do not have an establishment in the EU) if they offer goods or services to, or monitor the behavior of, data subjects located in the EU, irrespective of their nationality and the company's location.

The CCPA applies to organizations **"doing business in California."** This criterion is not precisely defined in the CCPA. However, according to the California Franchise Tax Board, doing business in California consists of "actively engaging in any transaction for the purpose of financial or pecuniary gain or profit" and an out-of-state entity can be considered as doing business in California if it meets certain thresholds (see Section 23101 of the Revenue and Taxation Code). Therefore, it is conceivable that out-of-state entities collecting, selling or disclosing personal information of California residents can fall under the scope of the CCPA.

The obligations imposed on businesses by the CCPA do not restrict a business's ability to "collect or sell a consumer's personal information if every aspect of that commercial conduct takes place wholly outside of California [...] Commercial conduct takes place wholly outside of California if the business collected that information while the consumer was outside of California, no part of the sale of the consumer's personal information occurred in California and no personal information collected while the consumer was in California was sold."



Fairly consistent

1.3. Material scope

The GDPR applies to the processing of personal data by automated means or non-automated means if the data is part of a filing system. The CCPA does not specifically delineate a material scope, but its obligations cover "collecting," "selling" or "sharing" personal information.

The CCPA definition of personal information presents some overlaps with the GDPR definition of personal data. The GDPR excludes from its application the processing of "anonymous data," while the CCPA excludes from its application collection, sharing or processing of "aggregate consumer information" and "deidentified data."

Unlike the GDPR, the CCPA provides several specific carve-outs from its scope of application, such as medical information and protected health information, publicly available information and employee information. The CCPA also excludes the transfer of data to a third party in the context of a merger from the definition of "selling" personal information. However, the CCPA still allows the right to opt-out if the resulting entity uses that personal information in a manner that is materially inconsistent with "the promises made at the time of collection."

Both the CCPA and the GDPR are not applicable in the law enforcement and national security areas, although they may apply to businesses providing services to law enforcement or national security agencies.

The GDPR does not apply in the context of a purely personal or household activity, whilst the CCPA does not apply to non-commercial activities. However, the GDPR exemption only refers to individuals, while the CCPA exemption covers businesses.

GDPR	CCPA
Articles 2, 4(1), 4(2), 4(6) Recitals 15-21, 26	Sections 1798.140(e),(o),(t),(q), 1798.145

Similarities

The GDPR applies to the "processing" of personal data. The definition of "processing" covers "any operation" performed on personal data "such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction."

Some of the CCPA obligations apply to "collecting" personal information and some apply to "selling" or sharing it.

- "Collecting" under the CCPA is "buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means." Therefore, it covers any type of operation by which a business acquires personal information, be it directly from the consumer, or indirectly (e.g. through observation).
- "Selling" includes "renting, disclosing, releasing, disseminating, making available, transferring, or otherwise communicating personal information for monetary or other valuable consideration." Note that selling does not necessarily involve a payment to be made in exchange for personal information.
- The CCPA's definition of "processing" is "any operation or set of operations that are performed on personal data" by either automated or not automated means. However, the term "processing" is only used in the definitions section.

Similarities (cont'd)

"**Personal data**" comprises "any information" that directly or indirectly relates to an identified or identifiable individual.

Anonymous data is specifically outside the scope of the GDPR. Anonymous data is information that does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.

The GDPR **excludes** from its application **processing of personal data by individuals for purely personal or household purposes**. This is data processing that has "no connection to a professional or commercial activity."

"**Personal information**" comprises "information" that directly or indirectly relates to, is reasonably capable of being associated with, or could reasonably be linked to a particular consumer or household. Businesses do not have to apply the CCPA obligations to "aggregate consumer information," which is defined as information that relates to a group or category of consumers, from which individual consumer identities have been removed, that is not linked or reasonably linkable to any consumer or household, including via a device. Businesses are also **exempted** from applying CCPA obligations to "**deidentified**" information, which is information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, provided that a business that uses deidentified information puts in place some technical and organizational measures to prevent reidentification.

The CCPA stipulates that the rights afforded and the obligations imposed on **businesses do not apply** if they are related to the **non-commercial activities** of a person.

Differences

The GDPR applies to the "processing of personal data" regardless of the type of processing operation, with the exception of the two types of processing listed below.

The GDPR **does not exclude specific categories of personal data** from its scope of application.

The CCPA primarily creates requirements for businesses that share or sell information, with some requirements that are also triggered by collection of information. For example, the **right to opt-out** is only available in the case of selling or sharing personal information, but not for merely collecting it.

The CCPA **specifically excludes** from its scope of application collecting and sharing of some categories of personal information:

- **employee data**, including information collected from a person in the course of acting as an employee or job applicant with a business (operable until 1 January 2021).
- **medical information** and protected health information that are covered by the Confidentiality of Medical Information Act and the Health Insurance Portability and Accountability Act;
- **information collected as part of a clinical trial**;
- **sale of information to or from consumer reporting agencies**;
- personal information under the **Gramm-Leach-Bliley Act**;

Differences (cont'd)

There are two types of processing activities that are excluded from the scope of the GDPR: **processing conducted through non-automated means that are not part of a filing system** and **processing conducted by a natural person for a purely personal or household purpose**.

- personal information under the **Driver's Privacy Protection Act**;
- **publicly available personal information**, which is defined as information that is lawfully made available from federal, state, or local government records.

The CCPA also excludes several specific processing activities from the definition of "**selling**", including:

- where a consumer uses or directs a business to intentionally disclose **personal information to a third party, via one or more deliberate interactions**. "**Hovering over, muting, pausing, or closing a given piece of content does not constitute a consumer's intent to interact with a third party**";
- **sharing with third parties an identifier that signals a consumer opted-out** from selling data;
- where a business shares **personal information with a service provider that is necessary for a "business purpose"** as defined in the CCPA; and
- where the business transfers the personal information to a third party as **an asset that is part of a merger, acquisition, bankruptcy, or other similar transaction**. However, if the third party materially alters how it uses the personal information in a manner that is materially inconsistent with the promises made at the time of collection, the right to opt-out still applies.

2. Key definitions



Fairly consistent

2.1. Personal data (personal information)

"Personal data" under the GDPR and "personal information" under the CCPA are both broadly defined.

The CCPA definition provides practical examples of what "any information" that relates to an identified or identifiable person means. For example, the CCPA definition refers to information relating to households in addition to information related to individuals. Whilst the definition of personal data in the GDPR only explicitly refers to individuals, there have been numerous discussions and enforcement action across Europe showing that personal data, as defined in the law, may also cover households.

Although the GDPR does not address inferences explicitly, while the CCPA does, they are subject to its requirements as long as they relate to identified or identifiable individuals, according to the definition of "personal data."

Unlike the CCPA, the GDPR separately provides a definition of sensitive data ("special categories of data") and prohibits processing of such data, unless one of the specific exemptions applies.

The CCPA provides for a definition to "biometric data," which includes elements of the GDPR's definition of special categories of data, such as DNA, fingerprints, and iris scans. However, the CCPA does not create a more protective regime for this category of data.

While the GDPR protects data related to health to a higher degree, since it is considered one of the special categories of data, the CCPA excludes from its protection categories of medical information, as well as data related to health collected for clinical trials.

GDPR

Articles 4(1), 9
Recitals 26 - 30

CCPA

Section 1798.140(b),(o)

Similarities

"**Personal data**" is defined as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an **identifier** such as a name, an identification number, **location data**, an **online identifier** or **to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.**" The GDPR also explains in its recitals that in order to determine whether a person is identifiable, "account should be taken of all the means **reasonably likely to be used**, such as singling out, either by the controller or by another person" to identify the individual directly or indirectly.

In its recitals, the GDPR specifies that **online identifiers**

"**Personal information**" is defined as "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." The CCPA further clarifies that the categories of information it enumerates are not always personal information, but they become personal information if that information identifies, relates to, describes, is capable of being associated with, or could be **reasonably** linked, directly or indirectly, with a particular consumer or household.

The CCPA provides specific categories of information that may

Similarities (cont'd)

may be considered as personal data, such as **IP addresses**, **cookie identifiers**, and **radio frequency identification tags**.

In Article 9, the GDPR also specifies the personal data that falls under special categories of personal data.

be "personal information," which include, but are not limited to:

- **identifiers** such as a real name, alias, postal address, unique personal identifier, online identifier IP address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers;
- **commercial information**, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies;
- **biometric information**;
- **internet or other electronic network activity information**, that includes browsing history, search history, and information regarding a consumer's interaction with an Internet Web site, application, or advertisement;
- **geolocation data**;
- **audio, electronic, visual, thermal, olfactory**, or similar information;
- **professional or employment related information**;
- **education information**, provided that it is not publicly available; and
- **inferences** drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

The GDPR does **not** apply to "**anonymised**" data, where the data can no longer identify the data subject.

The CCPA does **not** apply to "**deidentified**" information or "**aggregate**" consumer information. "**Deidentified**" means information that cannot reasonably identify or be linked, directly or indirectly, to a particular consumer. "**Aggregate**" consumer information is information that relates to a group or category of consumers, from which individual consumer identities have been removed, that is not linked or reasonably linkable to any consumer or household, including via a device.

Differences

"Personal data" under the GDPR covers **publicly available data**. Therefore, if a controller collects personal data from a publicly available source, the controller will be subject to the requirements laid down in the GDPR.

"Personal information" under the CCPA does **not** cover **publicly available information**, which is information that is lawfully made available from federal, state, or local government records. "Publicly available" does not include biometric information collected by a business about a consumer

Differences (cont'd)

The GDPR prohibits processing of **special categories of personal data**, which is "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the 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." However, the GDPR provides for exceptions to the prohibition of processing "sensitive data" in certain circumstances. The GDPR defines **biometric data** as "personal data resulting from specific technical processes related to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data." **Genetic data** is defined separately as "personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question."

The GDPR **protects personal data related to health** to a higher standard, since it is one of the special categories of data.

without the consumer's knowledge. Therefore, such information is covered by the obligations under the CCPA.

The CCPA does not separately define nor categorise "**sensitive data**" or "special categories of personal data." The CCPA defines **biometric data** as "an individual's physiological, biological or behavioral characteristics, **including an individual's deoxyribonucleic acid (DNA)**, that can be used, singly or in combination with each other or with other identifying data, to establish individual identity. Biometric information includes, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information." However, the CCPA does not provide special rules for collecting and sharing biometric data. They seem to only be relevant to indicate that such data can also be personal information, as well as to indicate that the exception of "publicly available information" does not include biometric data collected by businesses without the permission of consumers.

The CCPA **excludes medical information** from its protection, to the extent it is governed by the Confidentiality of Medical Information Act. It also excludes protected health information that is collected by a covered entity or business associate governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, established pursuant to the Health Insurance Portability and Accountability Act. In addition, it excludes information collected for clinical trials purposes subject to the Federal Policy for the Protection of Human Subjects, which would also include data related to health.

Additionally, the CCPA excludes employee data (this exception is operative until 1 January, 2021), which includes information collected from a person acting as an applicant, employee, owner, director, officer, medical staff member, or contractor of that business to the extent that the person's personal information is collected and used by a business solely within the context of the person's role as an applicant or employee of the business.



Fairly consistent

2.2. Pseudonymisation

The definition of "pseudonymisation" under the GDPR and CCPA is very similar in that it is the processing of personal data in such a manner that the personal data can no longer be attributed to an identified or identifiable person without the use of additional information, by putting in place technical and organizational measures which keep the additional information needed for identification separately.

Both the GDPR and the CCPA provide that controllers and businesses cannot be obliged to reidentify datasets in order to be able to comply with their obligations. However, the GDPR provides an exception to this rule concerning the rights of data subjects, to the extent that the additional information to reidentify the data is provided by the data subject himself or herself, while the CCPA specifically states that the rule also applies in the case of the right of access.

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

Similarities

"Pseudonymisation" is the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

"Pseudonymization" is the processing of personal information in a manner that renders the personal information no longer attributable to a specific consumer without the use of additional information, provided that the additional information is kept separately and is subject to technical and organizational measures to ensure that the personal information is not attributed to an identified or identifiable consumer.

Under the GDPR, "personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered as information on an identifiable natural person."

The CCPA does not clearly state whether its obligations apply to personal information that has been pseudonymized.

The GDPR provides that the controller cannot be obliged to maintain, acquire or process **additional information in order to identify the data subject** for the sole purposes of complying with the GDPR, if the purposes of that processing do not or do no longer require the identification of a data subject by the controller.

The CCPA provides that its rules cannot be construed "to require a business to **reidentify** or otherwise link information that is not maintained in a manner that would be considered personal information."

Differences

The GDPR provides that the **only instance** where the controller has to **reidentify** a dataset is where the data subject provides the additional information enabling his or her identification in order for the controller to be able to comply with **requests for the rights of the data subject**.

The CCPA provides that, in the case of the right of consumers to request that a business disclose the categories and specific pieces of information it has collected, that business is **not required to reidentify or otherwise link information that is not maintained in a manner that would be considered personal information**.



Fairly consistent

2.3. Controllers and processors (businesses and service providers)

"Controllers" under the GDPR bear similarity with "businesses" under the CCPA, as both are responsible for complying with the obligations under the respective laws. Some of the obligations of the GDPR, nonetheless, also apply to "processors," which are entities that process personal data on behalf of controllers and under the direction of controllers.

Although "processors" under the GDPR also bear similarity to "service providers" under the CCPA, when compared to the CCPA, the GDPR places more direct and detailed obligations on processors.

The GDPR requires a detailed contract or other legal act to be put in place between controllers and processors, laying out the mandate given to processors and other terms of the controller-processor relationship. Similarly, the CCPA requires that personal information is disclosed to service providers pursuant to a written contract.

GDPR	CCPA
Articles 4, 17, 28, 30, 32, 33, 35, 37, 38 Recitals 90, 93	Sections 1798.105, 1798.140, 1798.145, 1798.155

Similarities

A **data controller** is a natural or legal person, public authority, agency or other body that determines the **purposes** and **means** of the processing of personal data, alone or jointly with others.

A **business** is a **for-profit entity** that determines the **purposes** and **means** of the processing of consumers' personal information, **doing business in California** (see *Personal scope* and *Territorial scope* sections of this Guide).

A **data processor** is a natural or legal person, public authority, agency or other body which processes personal data **on behalf** of the controller.

A **service provider** is a for-profit entity that processes information **on behalf** of a CCPA-covered business.

Data processor activities must be governed by a **binding contract** or **other legal act** with regard to the controller. The contract should set out the subject matter, duration, nature and purpose of the processing, the types of personal data processed, the security measures, and the obligations and rights of the controller. Processors can only process personal data on instructions from the controller. Upon termination of the agreement with the controller, processors must return or destroy personal data at the choice of the controller. In addition, if the processor wants to engage another processor (sub-processor) it has to have the **written authorisation** of the data controller.

A business must disclose consumer's personal information for a business purpose pursuant to a **written contract**. The contract should prohibit the entity receiving the information from retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract.

Requirement under the "**right to erasure**" or "right to be forgotten":

- Data subjects have a right to request erasure to the controller as provided under Article 17

Requirement under "**right to deletion**":

- Upon a valid consumer's request to delete personal information, a business must direct **any service provider to delete consumers' personal information**.

Similarities (cont'd)

(see *Right to erasure* section of this Guide.)

- Upon a valid request for erasure, **controllers are obligated to take reasonable steps to have processors erase data.**

Generally, processors must support the controller to comply with data subjects' rights if required by the controller.

Liability and consequences of **non-compliance**:

- Data subjects have the right to bring an action against processors and **claim damages for "material or immaterial damage"** suffered as a result of an infringement of the processor obligations under the GDPR.
- Processors are only **liable for damage caused by processing in failure of their contractual obligations**

Liability for **misuse of personal information**:

- A service provider is liable for **civil penalties** if it uses the personal information received from businesses in violation of the CCPA.
- If a service provider fails to cure CCPA violations within 30 days, it is liable for a civil penalty under laws relating to **unfair competition** in an action brought by the Attorney General.

Differences

Other obligations imposed on processors:

- **Keep record of data processing activities:** processors are required to maintain a record of data processing activities in certain situations, including if the processor has 250 or more employees or if it processes data that is likely to result in a risk to the rights and freedoms of data subjects. The record should contain the categories of processing and any data transfers outside of the European Economic Area.
- **Implement appropriate technical and organisational measures:** processors must ensure security for processing data, which could include encryption or pseudonymization practices.
- **Data Protection Impact Assessment:** processors should assist the controller to undertake data protection impact assessments prior to the processing.
- **Appointing a DPO (Data Protection Officer):** processors must designate a data protection officer when required by the law, including where the processor processes personal data on a large scale.
- **Notify the controller of any data breach:** processors are required to notify the controller of any breach without undue delay after becoming aware of a breach.

For a business to not be considered as "selling" personal information when it shares it with a service provider for a business purpose, the service provider **must not further collect, sell, or use the personal information of the consumer except as necessary to perform the business purpose.**



Fairly consistent

2.4. Children

The GDPR emphasizes special protection for children and provides specific provisions for protecting children's personal data when processed for providing information society services. The CCPA creates a special rule for children with regard to "selling" personal information, however this rule is not limited to information society services.

Under the GDPR, children under 16 must have their parents' or guardians' consent on their behalf, with Member States being allowed to lower that age to 13. By contrast, the CCPA introduces an opt-in requirement for selling personal information of minors between 13 and 16 years old, while parents or legal guardians are required to opt-in for minors under 13.

Another important nuance is that the CCPA allows children personal information to be "sold" only on the basis of consent, unlike the GDPR, which allows other lawful grounds than consent to be applicable for processing of children data.

GDPR	CCPA
Articles 6, 8, 12, 40, 57 Recitals 38, 58, 75	Section 1798.120(c)

Similarities

The GDPR does not define "child," although it recognizes children as "vulnerable natural persons" that merit specific protection with regard to their personal data. Specific protection should apply when children's personal data is used for marketing or collected for services offered directly to a child.

Where the processing is based on consent, consent of a parent or guardian is required for providing information society services to a child below the **age of 16**. EU Member States can decide to lower the age, which may be no lower than **13**. Controllers are required to make **reasonable efforts** to verify that consent is given or authorised by a parent or guardian. However, the consent of the holder of parental responsibility should not be necessary in the context of preventative or counseling services offered directly to a child.

The CCPA does not define "child." The CCPA, however, ensures opt-in rights for minors under the age of 16.

Businesses must have opt-in consent to sell personal information of consumers under the **age of 16** if businesses have "actual knowledge" that a consumer is under 16. For consumers under the age of 13, the child's parent or guardian must affirmatively authorize the sale of the child's personal information. A business is deemed to have had **actual knowledge** of a child's age if it "**willfully disregards**" a child's age.

Differences

The GDPR does not provide for any exception for a controller that is **not aware** that it provides services to a child. It is not clear whether the consent requirement will apply if the child's personal data is unintentionally collected online.

When any information is addressed specifically to a child, controllers must take **appropriate measures** to provide **information** relating to processing in a concise, transparent, intelligible and easily accessible form, using clear and plain language, that the child can easily understand.

The CCPA provides for an **exception** for businesses that did not have actual knowledge of a child's age.



2.5. Research

The GDPR has specific provisions for processing of personal data for "historical or scientific research," as well as for "statistical purposes," and it indicates in its recitals that scientific research should be interpreted in a "broad manner." The GDPR provides for exceptions in this field, which include specific requirements regarding the lawful basis for processing, considering that processing for scientific research purposes is compatible with processing for any initial purpose and can thus rely on the lawful ground for that initial purpose, and a specific exception to the right of erasure. Member States are allowed to provide for derogations from the rights of the data subject where personal data are processed for scientific or historical research purposes.

The CCPA also defines research in a broad manner and it specifically mentions that processing of consumer data obtained in the course of providing a service can be further processed for research, since it will be considered compatible with the initial business purpose. However, the CCPA does not have an overarching purpose limitation principle that significantly limits the purposes for which personal information can be used by a business.

The GDPR requires that technical and organizational measures are put in place for processing of personal data for research purposes, with a focus on data minimization. Pseudonymization is offered as an example. Likewise, the CCPA requires safeguards to be put in place, but it provides a detailed list of such measures.

While the GDPR applies to clinical trials, the CCPA excludes clinical trials from its scope of application.

GDPR	CCPA
Articles 5(1)(b), 9(2)(j), 14(5), 17(3), 89 Recitals 33, 159, 160, 161	Sections 1798.105(d)(6), 1798.140(d)(6), (s), (t)(C)(ii)

Similarities

"**Scientific research** should be interpreted in a **broad manner**" and it should include technological development and demonstration, fundamental research, applied research, privately funded research and studies conducted in the public interest in the area of public health. The GDPR also refers to "historical research," which should also include research for genealogical purposes.

Article 5(1)(b) of the GDPR requires that personal data shall be collected for specified, explicit and legitimate purposes and **not further processed for incompatible purposes**. However, it also specifies that further processing for scientific or historical research purposes "shall not be considered incompatible" with the original purpose.

The GDPR provides that processing for research purposes must

"**Research**" is defined as scientific, systematic study and observation, including basic research or applied research that is in the public interest and that adheres to all other applicable ethics and privacy laws or studies conducted in the public interest in the area of public health.

Research with personal information that may have been collected from a consumer in the course of the consumer's interactions with a business's service or device **for other purposes is considered compatible** with the business purpose for which the personal information was collected.

The CCPA imposes specific safeguards for research conducted

Similarities (cont'd)

be subject to "**appropriate safeguards**" for the rights of the data subject, which shall ensure that technical and organizational measures are put in place in particular to ensure **data minimization**. **Pseudonymisation** is given as an example of such measures.

on consumer information collected initially for other purposes, such as that the personal information:

- should be subsequently **pseudonymized and deidentified**;
- should be made subject to **technical safeguards** that prohibit reidentification of the consumer to whom the information may pertain; there is a specific requirement that it should be subject to **additional security controls** that allow access to this information only on a need-to-know basis;
- should be made subject to business processes that specifically **prohibit reidentification of the information and protected from any reidentification attempts**;
- should be made subject to business processes to **prevent inadvertent release of deidentified information**;
- should be used **solely for research purposes that are compatible** with the context in which the personal information was collected; and
- **not** be used for any **commercial purpose**.

The **right to erasure** does **not** apply to the extent that the processing is necessary for scientific or historical research purposes if erasure "is likely to render impossible or seriously impair the achievement of the objectives of that processing."

The CCPA provides for a **research exception for deletion**, "when the businesses' deletion of the information is likely to render impossible or seriously impair the achievement of such research, if the consumer has provided informed consent."

Differences

One of the permissible uses of **special categories of personal data**, other than on the basis of consent of the data subject, is where processing is necessary for scientific or historical research purposes on the basis of Union or Member State law, which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Undertaking internal research for technological development and demonstration is considered a "business purpose." Where a service provider uses personal information of a consumer because it is necessary to perform a business purpose, such use is not considered "selling," and therefore consumers presumably cannot opt out of it.

The CCPA excludes clinical trials from its scope of application.

GDPR Portal

The most comprehensive resource for the development and maintenance of your GDPR programme.

- Understand obligations and requirements across key topics and sectors
- Track developments regarding Member State implementation and regulatory guidance
- Apply expert intelligence to make business decisions
- Utilise GDPR specific checklists and templates

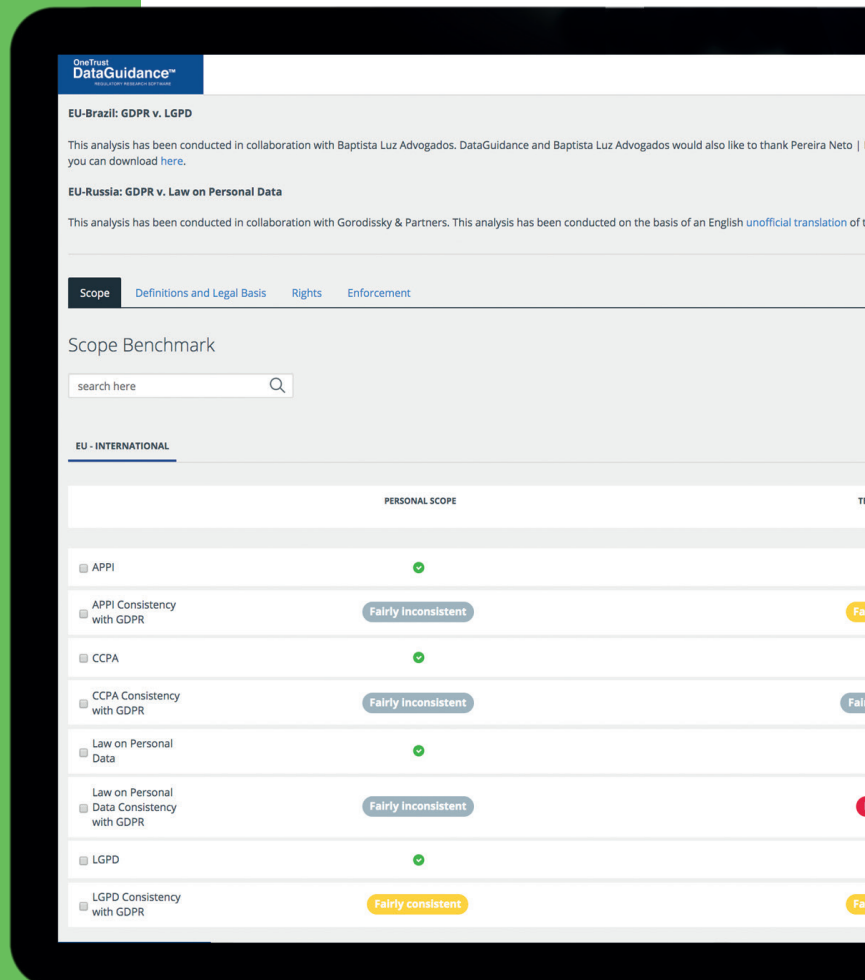
OneTrust DataGuidance

REGULATORY

Global Regulatory

40 In-House Legal Researchers, 50

Monitor regulatory developments and achieve global compliance



Sign up for a free trial at dataguidance.com

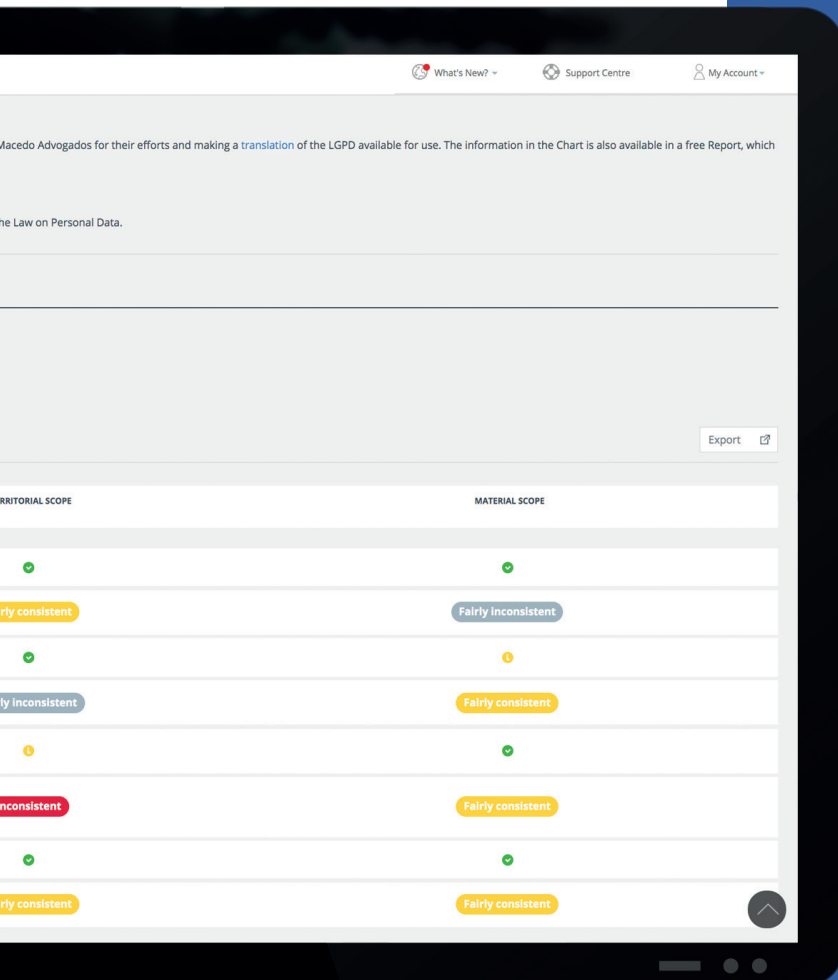
idance™

REGULATORY RESEARCH SOFTWARE

Research Software

1000+ Lawyers Across 300 Jurisdictions

Developments, mitigate risk
Global compliance.



GDPR Benchmarking

Understand and compare key provisions of the GDPR with relevant data protection law from around the globe.

- Compare requirements under the GDPR to California, Japan, Brazil, Russia and Thailand with a dedicated comparative tool
- Employ topic specific guidance to develop your compliance activities
- Monitor news and access written opinion pieces on the most recent developments

OneTrust DataGuidance™
REGULATORY RESEARCH SOFTWARE



3. Legal basis



Inconsistent

The GDPR provides that the processing of personal data will only be lawful where one of the six grounds under Article 6 is fulfilled. The CCPA does not set a list of grounds that businesses must adhere to *a priori* to collecting, selling and disclosing personal information, and only provides for an *a posteriori* mechanism, namely allowing customers to opt-out to the sale and disclosure of their personal information or to ask for erasure of the information.

GDPR
Articles 5-10
Recitals 39-48

CCPA
Section 1798.120

Similarities

The GDPR provides data subjects with a right to **withdraw consent** at any time as well as a **right to object** if their personal data is processed on the basis of legitimate interest or performing of a task in the public interest.

The CCPA does not have a list of "positive" legal grounds required for collecting, selling or disclosing personal information. However, consumers may ask businesses **not to sell their personal data**. In case a consumer opts-out, the business will only be able to sell and/or disclose personal information if the consumer gives their explicit permission.

The GDPR entails special conditions for processing of personal data of **children** for information society services (see section on *Children* of this Guide), when such processing is based on consent.

The CCPA allows businesses to sell **minors'** data on the basis of consent (see section on *Children* of this Guide). However, this opt-in is only mandated for the sale of information, and is not required for the collection of information.

Differences

The GDPR states that data controllers **can only process personal data when there is a legal ground for it**. The legal grounds are: consent, or when processing is necessary for (i) the performance of a contract which the data subject is part of in order to take steps at the request of the data subject prior to the entering into a contract; (ii) compliance with legal obligations to which the data controller is subject; (iii) to protect the vital interest of the data subject or of another natural person; (iv) performance carried out in the public interest or in the official authority vested in the data controller; or (v) for the legitimate interest of the data controller when this does not override the fundamental rights of the data subject. Further permissible uses are provided for the processing of special categories of personal data under Article 9(2). As a general rule, the processing of special categories of personal data is restricted unless an exemption applies.

The CCPA **does not list the legal grounds** on the basis of which businesses can collect and sell personal information. It only provides that businesses must obtain the consent of consumers when they enter into a scheme that gives **financial incentives** on the basis of the personal information provided.

4. Rights



4.1. Right to erasure (right to deletion)

Both the GDPR and the CCPA allow individuals to request the deletion of their personal information, unless exceptions apply. Under the CCPA, the right to deletion applies to personal information that has been "collected" from the consumer. The core of this right is quite similar in both pieces of legislation, however, its scope, applicability and exemptions vary. It is worth noting that some exceptions are the same under both laws, for example: freedom of speech, processing of personal data for research purposes if erasure of that data would impair the objectives of the research and establishing or exercising legal claims.

GDPR	CCPA
Articles 12, 17 Recitals 59, 65-66	Sections 1798.105, 1798.130(a), 1798.145 (g)(3)

Similarities

The scope of this right is not limited to the data controller, but also impacts **third parties**, such as recipients, data processors and sub-processors that may have to comply with erasure requests.

This right can be exercised **free of charge**. There may be some instances where a fee may be requested, notably when the requests are unfounded, excessive or have a repetitive character.

The GDPR specifies that data controllers must have in place **mechanisms** to ensure that the request is made by the data subject whose personal data is to be deleted.

Data subjects must be informed that they are entitled to ask for their data to be erased.

Exceptions: among the exceptions to the right of erasure provided by the GDPR are:

- **freedom of expression** (free speech), freedom of information;
- processing for **research purposes** of personal data that, if erased, would impair the objectives of the research;
- **establishment, exercise or defence of legal claims**; and
- for **complying with a legal obligation**.

The scope of this right is not limited to the business that collects personal data but also impacts **third parties** to whom data has been sold/passed on.

This right can be exercised **free of charge**. There may be some instances where a fee may be requested, notably when the requests are unfounded, excessive or have a repetitive character.

The CCPA specifies that businesses must have in place **mechanisms** to ensure that the request is made by the consumer whose personal information is to be deleted.

The privacy notice must inform consumers that they are entitled to ask for the deletion of their personal information.

Exceptions: among exceptions to the right of deletion provided by the CCPA are:

- **free speech or another right provided by law**;
- processing for **research purposes**, if the deletion of personal information would render impossible or seriously impair the achievement of such research;
- processing of that personal information is necessary to protect against **illegal activity or prosecute those responsible for the activity**; and
- for complying with a **legal obligation**.

Differences

The right to erasure only applies if any of the following grounds apply, such as where consent is withdrawn and there is no other legal ground for processing, or when personal data is no longer necessary for the purpose for which it was collected.

Data subjects' requests under this right must be replied to without "undue delay and in any event within **1 month** from the receipt of the request." The deadline can be extended to **2 additional months** taking into account the complexity and number of requests. In any case, the data subject must be informed of such extension within one month from the receipt of the request.

Methods to submit a request include **writing, orally and by other means which include electronic means** when appropriate.

If the controller has made the personal data public, controller must take "reasonable steps, including technical measures," to inform other controllers that are processing the personal data that the data subject has requested the erasure of any links to, or copy or replication of, those personal data.

Exemptions: in addition to the exceptions enumerated under "Similarities", a data controller is also exempted to comply with erasure requests for reasons of **public interest in the area of public health**.

The CCPA does not limit the scope of this right to specific situations, categories of personal information or purposes. The right generally applies to personal information that a business has collected from the consumer and it seems that the consumer does not have to justify his or her request.

The deadline to respond to a right request is **45 days** from the receipt of the consumer's request. The deadline can be extended an **additional 45 days** when reasonably necessary, if the consumer is informed within the first 45 days, according to Section 1798.130(a). **However**, there seems to be an inconsistency in the current text of the law. In another provision, which generally refers to exceptions to the law (Section 1798.145), the CCPA states that "the time period to respond to any verified consumer request may be extended by up to **90 additional days** where necessary, taking into account the complexity and number of the requests."

The CCPA states that at least two or more designated methods for submitting requests must be provided by the business including, at a minimum, a toll-free telephone number, and if the business maintains an internet website, a website address.

Exemptions: in addition to the exceptions enumerated under "Similarities", a business is not required to comply in the following circumstances:

- to perform a **contract between the business and the consumer**;
- **detect security incidents**, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for that activity;

Differences (cont'd)

- debug to identify and repair errors that impair existing intended functionality;
- to enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business;
- otherwise use the consumer's personal information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information;
- fulfill the terms of a written warranty or product recall conducted in accordance with federal law; and
- where personal information reflects a written or verbal communication or a transaction between the business and the consumer, where the consumer is a natural person who is acting as an employee, owner, director, officer, or contractor of a company, partnership, sole proprietorship, nonprofit, or government agency and whose communications or transaction with the business occur solely within the context of the business conducting due diligence regarding providing, or receiving a product or service to or from such company, partnership, sole proprietorship, nonprofit, or government agency.



4.2. Right to be informed

Both the GDPR and the CCPA include prescriptive provisions with regard to the information organizations must provide to individuals when collecting and processing their personal information. In particular, both pieces of legislation prescribe when information must be given to the individuals and what they must be informed of.

Unlike the GDPR, the CCPA does not distinguish between the notice for collecting information directly from individuals and the notice when information is obtained from other sources.

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

Similarities

The GDPR states that information on the following must be provided to individuals:

- the **categories** of personal data processed;
- the **purposes** of processing; and
- the **existence of data subjects' rights** and the contact details of the data protection officer.

The GDPR states that information must be provided to data subjects by controllers at the time when **personal data are obtained, when the personal data is collected directly from data subjects.**

Data controllers **cannot** collect and process personal data for purposes other than the ones about which the consumers were informed, unless they provide them with further information.

The CCPA states that information on the following must be provided to individuals:

- the **categories** of personal information to be collected;
- the **purposes** for which collected personal information is used; and
- if a business sells personal information about the consumer to third parties, the rights of the consumers and the methods to exercise such rights must be given to consumers. This includes a link to the '**Do Not Sell My Personal Information**' page where consumers can exercise their right to opt-out.

A business is exempted from the obligation to provide notice if the personal information processed reflects a written or verbal communication or a transaction between the business and the consumer, when the consumer is an employee or a natural person acting as contractor for an organization such as a business, not for profit or government agency. This exception only operates until 1 January 2021.

The CCPA states that businesses must inform customers **before or at the point of collection.**

Businesses **cannot** collect additional personal information without telling the consumers what information is collected and for which purpose, unless they provide them with further information.

Differences

The GDPR also states that information on the following must be provided to individuals:

- identity of the controller;
- contact details of the data protection officer;
- the legitimate interest of the data controller or the third party;
- the recipients or categories of personal data;
- transfer of data to third parties;
- data retention period;
- the right to withdraw consent at any time;
- the right to lodge a complaint with a supervisory authority.
- when data is necessary for the performance of a contract, the possible consequences of not doing so; and
- the existence of automated decision-making including profiling, including the logic involved and consequences of such processing.

The GDPR provides specific information that must be given to the data subject **when their data is collected by a third party**, which include the sources from which data was collected. Notice must be given within a reasonable period after obtaining the data, but at the latest within one month; or at the time of the first communication with the data subject; or at the latest when personal data are first disclosed to a recipient.

The CCPA also states that information on the following must be provided to individuals:

- the categories of personal information collected/sold/disclosed for business purposes in the previous 12 months; and
- alternatively, if no personal information was sold, that should be written in the privacy policy.

There is a specific requirement that consumers receive "**explicit notice**" when a third party intends to sell personal information about that consumer that has been sold to the third party by a business.

The CCPA specifies that the **privacy policy must be updated every 12 months**.



4.3. Right to object (right to opt-out)

Both the GDPR and the CCPA guarantee a right for individuals to ask organizations to cease the processing, and selling respectively, of their data.

The CCPA requires that a link with the title "Do Not Sell My Personal Information" is provided on the homepage of the business. Additionally, the CCPA provides that any third party that received personal information pursuant to their "selling" can only further sell that personal information if consumers are provided "explicit notice" and the opportunity to opt-out of this subsequent "selling."

Under the CCPA, consumers can only opt-out of the sale of personal data, and not the collection or other uses that do not fall under the definition of "selling." By contrast, individuals can object to any type of processing of personal data under the GDPR – either by simply withdrawing consent, or by objecting to processing that is based on legitimate interest, or on necessity for a task in the public interest.

The CCPA right to opt-out of personal information is absolute, similar to the GDPR absolute right to object to direct marketing. While the CCPA does not provide at all for a general right to opt-out of processing, the GDPR general right to object to processing other than for direct marketing has a specific exception where the controller demonstrates compelling legitimate grounds for the processing that override the rights and interests of the data subject.

GDPR	CCPA
Articles 12, 21 Recital 70	Sections 1798.120, 1798.135

Similarities

Data subjects have several ways to opt-out of processing of their personal data:

- they can **withdraw consent**;
- they can **exercise the general right to object** to processing that is based on legitimate interests or on a task carried out in the public interest; or
- they can **object to processing of their data for direct marketing purposes**.

Information about this right and on how to exercise it must be included in the **privacy notice**. In particular, in the context of direct marketing, opting-out must be as easy as opting-in.

Consumers have the right to **opt-out from selling of their personal information**. They also have the right to opt-out from the subsequent selling of their personal information by a third party that received personal information after an initial "selling." The third party shall not sell the personal information unless the consumer has received "explicit notice" and is provided an opportunity to opt-out.

If a business sells consumers' personal information, information about this right must be given to consumers in the **privacy notice**. Moreover, a **link to the page 'Do Not Sell My Personal Information'** must be included in the homepage of the business. The CCPA allows businesses to create a dedicated homepage for California consumers.

Differences

The GDPR provides data subjects with the **right to object** to the processing of their personal data when the processing is based on the legitimate interest of the controller or a third party. The data controller would have to cease processing personal data unless it demonstrates that there are compelling legitimate grounds to continue the processing. Moreover, the data subject has the right to object to processing for direct marketing as well as to withdraw consent at any time.

The GDPR does **not** prescribe the specific language to be used.

The CCPA provides consumers with a right to opt-out from the selling and/or disclosing for business purposes of their personal information. The opt-out can therefore only stop the selling of personal information, and it does not impact other uses of their information. However, the right to opt-out of the sale is **absolute**, in the sense that businesses cannot reject an opt-out request on the basis of their compelling legitimate grounds.

Businesses must adhere to the language provided in the CCPA, namely the homepage of their website must have a link titled '**Do Not Sell My Personal Information.**'

The right to opt out does not apply to vehicle information or vehicle ownership information retained or shared between a new motor vehicle dealer and the vehicle's manufacturer if the vehicle or ownership information is shared for the purpose of effectuating, or in anticipation of effectuating, a vehicle repair covered by a vehicle warranty or a recall provided that the new motor vehicle dealer or vehicle manufacturer with which that vehicle information or ownership information is shared does not sell, share, or use that information for any other purpose.



4.4. Right of access

Both the GDPR and the CCPA establish a right of access, which allows individuals to have full visibility of the data an organization holds about them: they can obtain details about the data being processed, but also copies of the data items themselves.

The two laws present some differences, for example, in relation to the procedure organizations should follow to comply with an individual's request. In addition, the CCPA provides that whenever access is granted to consumers electronically, the information must be in a portable and, to the extent possible, readily useable format that allows the consumer to transmit the information to another entity.

GDPR	CCPA
Articles 12, 15, 20 Recitals 59, 63, 64	Sections 1798.100, 1798.110, 1798.130, 1798.145 (g)(3)

Similarities

The GDPR states that, when responding to an access request, a data controller must indicate the **purposes** of the processing; the **categories of personal data** concerned; the **recipients or categories of recipients** to whom personal data have been disclosed to; and **any sources** from which data was collected. The GDPR specifies that individuals also have the right to receive a **copy** of the personal data processed about them.

Data subjects must have a variety of means through which they can make their request, including through **electronic means and orally**. When the request is made through electronic means, the data controller should submit the response through the same means.

The GDPR specifies that data controllers must have in place **mechanisms** to ensure that the request is made by the data subject whose personal data is requested access to.

The GDPR states that data subjects can exercise this right **free of charge**. There may be some instances where a fee may be requested, notably when the requests are unfounded, excessive or have a repetitive character.

The CCPA states that, when responding to an access request, a business must indicate the **categories of personal information** collected/sold; the **categories of sources** from which the personal information is collected; the business or commercial **purpose** for collecting or selling personal information; and the **categories of third parties** with whom the business shares personal information. The CCPA specifies that individuals also have the right to be given access to the pieces of personal information collected about them.

Consumers must be given at least two methods to make their request to access their personal information, notably via a **toll-free phone or a webpage**. The business may send the response via mail or electronic means. A business that operates exclusively online and has a direct relationship with a consumer from whom it collects personal information shall only be required to provide an email address for submitting requests for information.

The CCPA specifies that businesses must have in place **mechanisms** to ensure that the request is made by the consumer whose personal information is requested access to.

Disclosure and delivery of personal information as required by the right of access must be **free of charge**. There may be some instances where a fee may be requested, notably when the requests are unfounded, excessive or have a repetitive character.

Differences

The right applies to all the personal data collected and processed about the data subject making the request.

Under the GDPR, the data controller must include further information in the response to a request of access, notably, the retention period, the right to lodge a complaint with the supervisory authority, the existence of automated decision making, and existence of data transfers.

Data controllers can refuse to act on a request when it is manifestly unfounded, excessive or has a repetitive character.

Data subjects' requests must be complied without "**undue delay** and in any event within **1 month** from the receipt of the request." The deadline can be extended an **additional 2 months** taking into account the complexity and number of requests. In any case, the data subject must be informed of such extension within one month from the receipt of the request.

The GDPR has a **distinct right to data portability**, which applies under its own specific conditions (see below).

The right applies **only** to personal information collected in the **12 months prior to the request**.

Businesses are not required to provide access to personal information more than twice in 12 months.

The deadline to respond to such a right is **45 days** of receipt of the consumer's request. It could be extended an **additional 45 days**, but notice should be given to the consumer within the first 45 days. However, there seems to be an inconsistency in the current text of the law that allows an extension to **90 days**, under a different provision (see *Right to erasure* section of this Guide).

The CCPA states that when businesses provide data electronically to the consumer this data should be sent in a **portable and readily usable format** that allows for the transmission of this data to **third parties**. The CCPA provides that this must be done only when technically feasible.

In addition, the CCPA provides that, until 1 January, 2021, the right of access does not apply when personal information reflects a written or verbal communication or a transaction between the business and the consumer, where the consumer is a natural person who is acting as an employee, owner, director, officer, or contractor of a company, partnership, sole proprietorship, nonprofit, or government agency and whose communications or transaction with the business occur solely within the context of the business conducting due diligence regarding, or providing or receiving a product or service to or from such company, partnership, sole proprietorship, nonprofit or government agency.



4.5. Right not to be subject to discrimination for the exercise of rights

The CCPA introduces the right not to be subject to discrimination for the exercise of rights under the CCPA. This right is not explicitly included in the GDPR, however, some provisions can be found in the GDPR that are based on the same principle.

GDPR
Articles 5, 22
Recitals 39, 71-73

CCPA
Section 1798.125

Similarities

The GDPR does **not include an explicit provision** stating that a data subject must not be discriminated on the basis of their choices on how to exercise their data protection rights. However, it is implicit from the principles of the GDPR that individuals must be protected from discriminatory consequences derived from the processing of their personal data. For example, Article 5 states that personal data must be processed 'fairly'; Article 13 states that data subjects must be informed of the consequences derived from automated decision-making; and Article 22 specifies that individuals have the right not to be subject to solely automated decision-making that has a legal or significant effect upon them. Additionally, the GDPR emphasizes that when processing is based on consent, in order for consent to be valid, it must be freely given. Consent is not considered freely given if the data subject has no genuine or free choice or is unable to refuse or "withdraw consent without detriment."

The CCPA states that consumers **must not be discriminated because of the exercise of their rights** under the CCPA.

Differences

GDPR

The GDPR does not explicitly include this right and therefore **no scope is defined**.

CCPA

The CCPA defines the scope of this right by stating that consumers must not be discriminated against because of the exercise of their rights under the CCPA, which means they must not be:

- **denied goods or services;**
- **charged different prices or rates for goods or services**, including through the use of discounts or other benefits or imposing penalties;
- **provided a different level or quality of goods or services;** and
- suggested they will receive a **different price or rate for goods or services**.

It has to be noted that businesses can set up schemes for providing **financial incentives**, but consumers must **opt-in** to become part of them.

4.6. Right to data portability



Both the GDPR and the CCPA recognize a right to data portability. The CCPA considers data portability as part of the right to access, while the GDPR provides for a separate and distinctive right.

GDPR
Articles 12, 20
Recital 68

CCPA
Sections 1798.100, 1798.110,
1798.130, 1798.145 (g)(3)

Similarities

Data subjects have the **right to receive their data processed on the basis of contract or consent in a "structured, commonly used, and machine-readable format"** and to transmit that data to another controller without hindrance.

The GDPR states that consumers can exercise this right **free of charge**. There may be some instances where a fee may be requested, notably when the requests are unfounded, excessive or have a repetitive character.

Data subjects must have a variety of means through which they can make their request, including through **electronic means and orally**. When the request is made through electronic means, the data controller should submit the response through the same means.

The GDPR specifies that data controllers must have in place **mechanisms** to ensure that the request is made by the data subject whose personal data is requested access to.

The GDPR provides that this must be done only when **technically feasible**.

The CCPA states that when businesses provide data electronically to the consumer following an access request this data should be sent in a **portable and readily usable format that allows for the transmission of this data to third parties** without hindrance.

The CCPA states that consumers can exercise this right **free of charge**. There may be some instances where a fee may be requested, notably when the requests are unfounded, excessive or have a repetitive character.

Consumers must be given at least two methods to make their request to access their personal information, notably via a **toll-free phone or a webpage**. The business may send the response via mail or electronic means.

The CCPA specifies that businesses must have in place **mechanisms** to ensure that the request is made by the consumer whose personal information is requested access to.

The CCPA provides that this must be done only when **technically feasible**.

Differences

The right to data portability **only** applies to the **personal data** that has been **provided by the data subject** themselves and that is processed on the basis of **consent** or **contract** and the processing is carried out by **automated means**.

Data controllers must respond without **undue delay** and in any event **within 1 month** of receipt of the request. It could be extended an **additional 2 months**, but notice should be given to the data subject within the first month.

In addition to having data subjects receive personal data under the right to data portability, the GDPR **extends this right to having the personal data transmitted directly from one controller to another**.

The right to data portability is an **extension of the right to access**, and therefore it is subject to the same limitation (e.g. it only applies to data collected in the previous 12 months).

Businesses must respond within **45 days** from receipt of the request. It could be extended an **additional 45 days**, but notice should be given to the consumer within the first 45 days. However, there seems to be an inconsistency in the current text of the law that allows an extension to **90 days**, under a different provision (see *Right to erasure* section of this Guide).

The CCPA's right is limited to allowing consumers receive personal information, and it does **not** extend to having a business transfer the information to another business.



MISSION

The mission of the Future of Privacy Forum is to serve as a catalyst for privacy leadership and scholarship, advancing principled data practices in support of emerging technologies.

WHO WE ARE

FPF brings together industry, academics, consumer advocates, and other thought leaders to explore the challenges posed by technological innovation and develop privacy protections, ethical norms, and workable business practices.

VISION

We believe that...

- Technological innovation and new uses of data can help solve big societal problems and improve lives.
- Technological innovation must be accompanied by responsible data practices.
- It is possible to build a world where technological innovation and privacy can coexist.
- It is possible to reach consensus on ethical norms, policies and business practices to address new privacy challenges.

OUR SUPPORTERS

FPF works with the privacy leaders at 175 companies and in partnership with leading academics and civil society organizations. We are supported by industry, charitable foundations and governments.

ENGAGE WITH US

Stay up-to-date on our work by following us at @futureofprivacy on social media. Visit our website and subscribe to our mailing list: <https://fpf.org/subscribe>.

5. Enforcement



5.1. Monetary penalties

Both the GDPR and the CCPA provide for the possibility for monetary penalties to be issued in cases of non-compliance. However, the nature of the penalties, the amount and the procedure to be followed differ quite significantly.

GDPR Articles 83, 84 Recitals 148 - 152	CCPA Section 1798.155
---	--------------------------

Similarities

The GDPR provides for **monetary penalties** in case of non-compliance.

The CCPA provides for **monetary penalties** in case of non-compliance.

Differences

Administrative fines can be directly issued by a data protection authority.

Civil penalties can be issued meaning that the penalty is issued by a court.

Depending on the violation occurred the penalty may be up to either:

- **2% of global annual turnover or €10 million**, whichever is higher; or
- **4% of global annual turnover or €20 million**, whichever is higher.

Depending on the violation occurred the penalty may be up to:

- **\$2,500** for each **violation**;
- **\$7,500** for each **intentional violation**.

The amount of the penalty may also vary depending on "the nature, gravity and duration of the infringement," the nature of the processing, the number of data subject affected, and the damages suffered, the negligent or intentional character of the infringement, etc., with a complete list in Article 83(2) of the GDPR.

CCPA does not provide for a maximum amount that can result for the imposition of several penalties for each violation.

The administrative fine can be imposed directly by the competent data protection authority taking into account that several data protection authorities may be involved if the violation involves more than one Member State.

Any violation of the CCPA is assessed and recovered in a civil action brought by the **Attorney General**.



Fairly inconsistent

5.2. Supervisory authority

Both the GDPR and the CCPA provide for an authority to supervise the application of the law and to assist organizations in understanding and complying with it. However, the two designated supervisory authorities, the Attorney General and the national data protection authorities under the CCPA and the GDPR respectively, have different investigatory and enforcement powers.

Additionally, it has to be noted that, in the European Union, national data protection authorities form part of the European Data Protection Board, a body that ensures the consistent application of the GDPR across Europe.

GDPR
Articles 51-84
Recitals 117 - 140

CCPA
Sections 1798.155, 1798.185

Similarities

Data protection authorities have the task to **promote awareness and produce guidance** on the GDPR.

The Attorney General is expected to create **regulations** "on, but not limited to," specific areas of the CCPA.

Differences

Data protection authorities have **investigatory powers** which include to: "conduct data protection audits, access all personal data necessary for the performance of its tasks, obtain access to any premises of the data controller and processor, including equipment and means."

The Attorney General has the power to **assess a violation** of the CCPA. The CCPA does not specify which activities are included in this assessment.

Data protection authorities have **corrective powers** which include: "issuing warnings, reprimands, to order the controller and processor to comply, order the controller to communicate a data breach to the data subject, impose a ban on processing, order the rectification or erasure of data, suspend the transfer of data and impose administrative fines."

The Attorney General has the power to assess alleged violations of the CCPA and to bring action before the court for civil penalties, which include **monetary penalties and injunctions**.

The GDPR does not regulate how data protection authorities are funded, this being left to the Member States to decide.

The monetary penalties collected through civil actions under the CCPA form the **Consumer Privacy Fund**, which funds the activities of the Attorney General in this sector.

The GDPR states that data protection authorities must act in "**complete independence when performing their tasks**," which also means that they must be free from financial control by having a separate and dedicated budget.

The Attorney General has the power to **independently start investigations** and actions against alleged non-compliance from businesses.



5.3. Civil remedies for individuals

Both the GDPR and the CCPA provide individuals with a cause of action to seek damages for privacy violations. In addition, both laws allow for class or collective actions to be brought against organizations.

However, it has to be noted that under the GDPR, an action can be brought for any violation of the law, while the CCPA provides a cause for action only with regard to the failure of security measures and in the context of data breaches.

GDPR
Articles 79 - 82
Recitals 141 -147

CCPA
Section 1798.150

Similarities

Both the GDPR and the CCPA provide individuals with a cause of action to seek damages for violation of privacy laws with regard to security measures violations and data breaches.

Both the GDPR and the CCPA provide individuals with a cause of action to seek damages for violation of privacy laws with regards to security measures violations and data breaches.

Differences

Any violation of the GDPR can trigger the claim for judicial remedies. Data subjects can claim both **material and non-material damages**.

This remedy is **only allowed** when non-encrypted or non-redacted personal information is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of security obligations.

The GDPR allows Member States to provide for the possibility for data subjects to give a mandate for representation to a non-for-profit association, association or organisation that has as its statutory objective the protection of data subject rights.

Prior to initiating any action against a business for statutory damages on an individual or class-wide basis, businesses are provided 30 days' written notice including a reference to the alleged violations. If the violation is "cured" within 30 days and no further violation is claimed, no action is initiated. The CCPA further states that "no notice shall be required prior to an individual consumer initiating an action solely for actual pecuniary damages suffered as a result of the alleged violations of this title. If a business continues to violate this title in breach of the express written statement provided to the consumer under this section, the consumer may initiate an action against the business to enforce the written statement and may pursue statutory damages for each breach of the express written statement, as well as any other violation of the title that postdates the written statement."

The GDPR does not provide any figure for potential damages.

The amount of damages is established by Statute. **Damages** could be in an amount not less than **\$100 and not greater than \$750** per consumer per incident or actual damages, whichever is greater.

Index: CCPA articles

- 1798.100 – Right of Access and Portability
- 1798.105 – Right to Deletion
- 1798.110 – Disclosure obligations (businesses that collect personal data)
- 1798.115 – Disclosure obligations (businesses that sell personal data)
- 1798.120 – Right to Opt Out
- 1798.125 – Prohibited discrimination and use of financial incentives
- 1798.130 – Compliance obligations with regards to consumers rights
- 1798.135 – Compliance obligations with regards to right to opt-out
- 1798.140 – Definitions
- 1798.145 – Exemptions
- 1798.150 – Consumer relief for Data Breaches
- 1798.155 – Enforcement
- 1798.160 – Consumer Privacy Fund
- 1798.175 – Application
- 1798.180 – State Preemption
- 1798.185 – Attorney General Regulations
- 1798.190 – Transactions
- 1798.192 – Void & Unenforceable Contracts or Agreements
- 1798.194 – Interpretation of Title
- 1798.196 – Preemption
- 1798.198 – Effective Date
- 1798.199 – Effective Date of State Preemption

