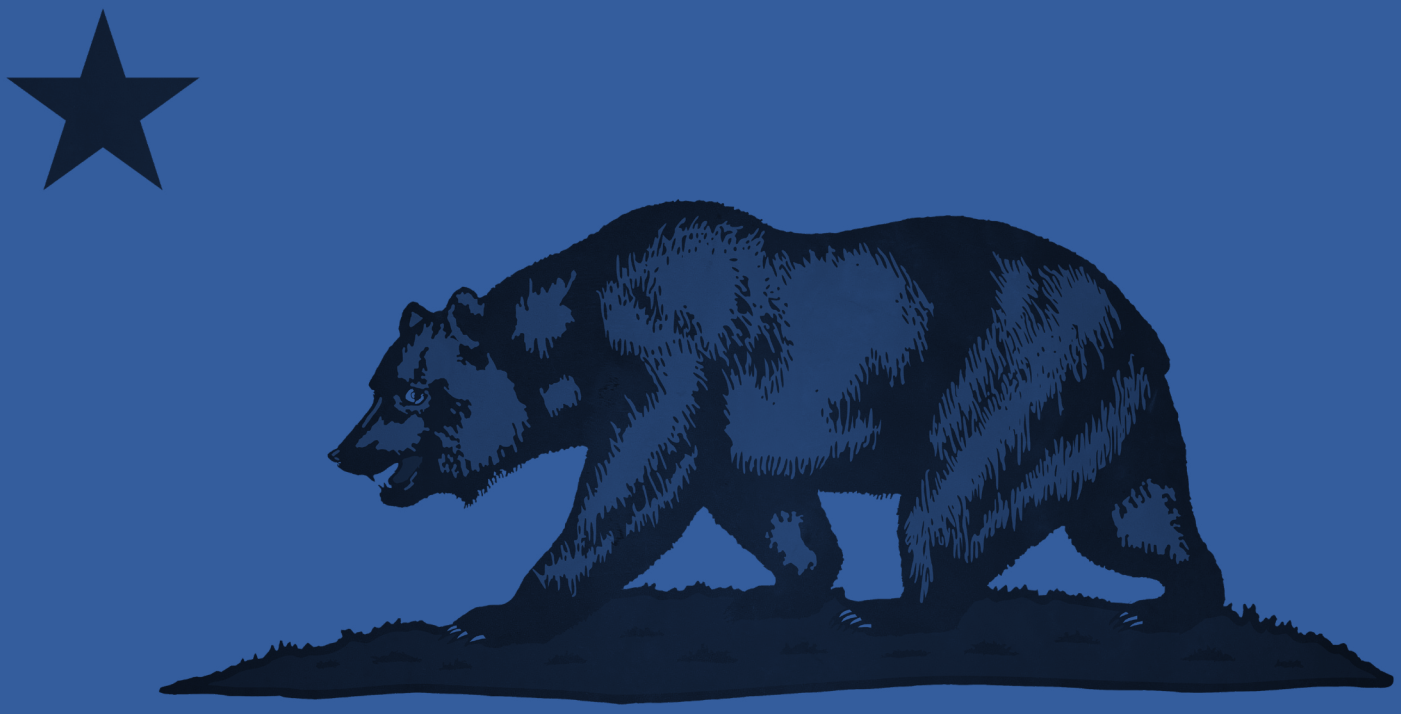


Comparing privacy laws:
GDPR v. CCPA & CPRA

January 2022

NEWMEYER DILLION

OneTrust DataGuidance™
REGULATORY RESEARCH SOFTWARE

About the authors

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

OneTrust DataGuidance™ Regulatory Research includes focused guidance around core topics (i.e. GDPR, data transfers, breach notification, among others), Comparisons 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 program.

Newmeyer & Dillion LLP is a full service law firm headquartered in Newport Beach, California, with additional offices located in Walnut Creek, California and Las Vegas, Nevada. Newmeyer Dillion's attorney roster is comprised of business-focused lawyers with a focus on the big picture, from business transactions and litigation to the forefront of technology, privacy, and the law, seeking to counsel clients holistically at every stage of their business and work side-by-side and hand in glove to create solutions at the best possible cost.

The attorneys of Newmeyer Dillion strive to be the kind of people you actually enjoy dealing with and the kind of law firm you are proud to call a partner. The business relationships become lifelong friendships and the friendships become lifelong business relationships.

Contributors

Newmeyer & Dillion LLP: Jeffrey Dennis, Kyle Janecek

OneTrust DataGuidance™: Iana Gaytandjieva, Angela Potter, Edidiong Udoh, Alexander Fetani, Marcello Ferraresi, Victoria Prescott

Image production credits:
Cover/p.3/p.43: Bulgac / Signature collection / istockphoto.com, cnythzl / Signature collection / istockphoto.com
Scale key p6-49: enisaksoy / Signature collection / istockphoto.com
Icon p.33-40: AlexeyBlogoodf / Essentials collection / istockphoto.com
Icon p.47-51: cnythzl / Signature collection / istockphoto.com | MicroStockHub / Signature collection / istockphoto.com

Table of contents

Should I be worried about an ADA website claim?

What exposure do I face if named in a cyber-based complaint?

What should I do if my company suffers a breach, or experiences ransomware?

How do we choose the right cyber insurance?

What privacy compliance frameworks impact my company, and how do I comply?

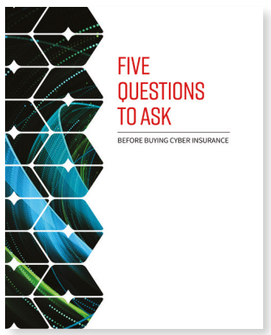
24/7 Data Breach Response / Ransomware Hotline

844.414.2333

TO FIND THE RIGHT ANSWERS, ASK THE RIGHT QUESTIONS

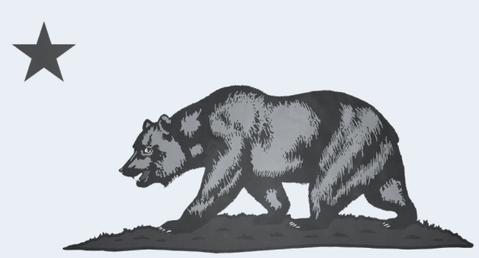
Your most pressing legal problems rarely have simple answers. That's why we ask before we act—about your business, your goals and your deepest concerns. For more than three decades, Newmeyer Dillion has used the answers to propel clients to success.

Download our free guide, *Five Questions to Ask Before Buying Cyber Insurance*, at newmeyerdillion.com/5questions-cyber.



Newport Beach | Walnut Creek | Las Vegas
newmeyerdillion.com

NEWMEYER DILLION



Introduction

Soon after the entry into effect of the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') on 25 May 2018, the California Consumer Privacy Act of 2018 ('CCPA') (under Sections 1798.100 *et seq.* of Title 1.81.5. of Part 4 of Division 3 of the California Civil Code ('Cal. Civ. Code')) was signed into law on 28 June 2019. The CCPA later entered into effect on 1 January 2020 and became enforceable from 1 July 2020. Both the GDPR and the CCPA aim to guarantee the protection of individuals' personal data and apply to businesses processing such data.

To date, the GDPR is one of the most comprehensive data protection laws, with several countries using it as inspiration to strengthen or establish laws on the protection of personal data. In the US, and absent a comprehensive federal framework, the CCPA is one of the most significant and strictest privacy laws, with a wide territorial application due to California being one of the largest global economies.

On 14 August 2020, the Final CCPA Regulations ('the CCPA Regulations'), which provide further requirements and clarifications on the application of the CCPA, were approved. Then on 15 March 2021, additional regulations to the CCPA were approved, further facilitating understanding of, and compliance with, the CCPA.

On 4 November 2020, the California Privacy Rights Act of 2020 ('CPRA'), or Proposition 24, passed the 2020 California General Elections. Although the CPRA became effective immediately, most of its provisions will not be operational until January 2023 and will not be enforced until July 2023. The CPRA has introduced a number of changes to the CCPA, such as new definitions, expanded consumer rights, and the establishment of the California Privacy Protection Agency ('CPPA'), among other important obligations for business.

Notably, the GDPR and CCPA are similar in certain aspects, such as with certain definitions, affording protections to individuals under the age of 16, and with the inclusion of various rights, such as the right to access personal information and the right to delete such data.

However, the laws diverge with respect to scope of application, provisions around limitations on the collection of personal information, and on certain obligations such as accountability. Moreover, while the GDPR requires a legal basis for the processing of personal data, the CCPA does not require the same. Furthermore, the CCPA provides for requirements around the selling of personal information, requiring that businesses include on their homepage a 'Do Not Sell My Personal Information' link, among various other differences.

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

Structure and overview of the Guide

This Guide provides a comparison of the two legislative frameworks on the following key provisions:

1. Scope
2. Key definitions
3. Legal basis
4. Controller and processor obligations
5. Individuals' rights
6. Enforcement

Each topic includes relevant provisions from the two legislative frameworks, a summary of the comparison, and a detailed analysis of the similarities and differences between the GDPR and the CCPA/CPRA (collectively, the 'California Privacy Laws').

Key for giving the consistency rate

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

Fairly consistent: The GDPR and the CCPA/CPRA 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 the CCPA/CPRA bear several differences with regard to the scope and application of the provision considered, however, its rationale and core presents some similarities.

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

Usage of the Guide

This Guide is general and informational 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.

1. Scope

1.1. Personal scope

While the definitions differ, the scope of the CCPA and the CPRA are similar to the GDPR in that the laws and regulations apply to natural persons. However, unlike the GDPR, the CCPA and CPRA do not include definitions for 'data controllers' or 'data processors' and instead apply to 'businesses' and 'service providers' outlining specific thresholds for the former.

GDPR	California Privacy Laws
Articles 3, 4(1) Recitals 2, 14, 22-25	Sections 1798.140 and 1798.145 of the CCPA Section 14 of the CPRA

Similarities

Article 4(1) of the GDPR clarifies that a '**data subject**' is 'an identified or identifiable natural person.'

The CCPA and CPRA protect **natural persons** who are California residents.

Differences

The GDPR **only** protects **living individuals**. The GDPR does not protect the personal data of deceased individuals, this being left to Member States to regulate.

The CCPA and CPRA **do not** address whether its protections extend to **deceased persons**.

The GDPR defines a '**data controller**' as a 'natural and legal person, public authority, agency or other body which, alone or jointly, with others, determines the purposes and means of the processing of personal data.'

The CCPA and CPRA **do not** define the term 'data controllers' but instead refer to '**businesses**'. Businesses are limited to sole proprietorships, partnerships, limited liability companies, corporations, associations or another legal entity that is organised or operated for profit, and doing business with California residents. This is coupled with a 'size minimum' of gross revenues in excess of **$25,000,000**, deriving **50%** of its annual revenue from the sale of personal information, or buying, selling, or sharing for commercial purposes, the personal information of 100,000 or more consumers or households under the CPRA (NB: the CCPA only requires personal information of 50,000 individuals or households, which will change under the CPRA from 1 January 2023).

While this definition may encompass entities that would also fall under the definition of a 'data controller', it greatly limits which entities are subject to the CCPA and CPRA.

The GDPR defines a '**data processor**' as a 'natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.'

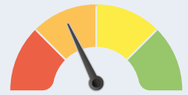
The CCPA and CPRA **do not** define the term 'data processors' but instead refer to '**service providers**'. This includes any person (including natural persons or legal entities). Notwithstanding this, service providers have certain restrictions on how information can be disclosed or otherwise utilised.

GDPR	California Privacy Legislation

Differences (cont'd)

	Further, there are additional subsets including '**contractors**' (who must have a contract with the entity collecting the information) and '**third parties**' who are defined as any party aside from the business collecting the data, contractors, or service providers.
The GDPR **applies** to data controllers and data processors who may be **public bodies**.	The CCPA/CPRA **do not** apply to **public bodies**.
The GDPR provides that it 'should apply to natural persons, **whatever their nationality or place of residence**, in relation to the processing of their personal data.'	The CCPA and CPRA are **limited solely to California residents and entities doing business in the state** of California, while activities that occur wholly outside of California fall outside of the purview of the CCPA and CPRA.

1.2. Territorial scope



Fairly inconsistent

The CCPA and CPRA are similar to the GDPR in that they apply to entities with a presence within the respective territories. The GDPR, however, applies to natural persons regardless of their nationality, whereas the CCPA and CPRA are more limited in scope, applying solely to California residents and entities doing business in the state of California.

GDPR Articles 3, 4, 11 Recitals 2, 14, 22-25	California Privacy Laws Section 1798.145 of the CCPA

Similarities

The GDPR **applies** to organisations that have presence in the EU. In particular under Article 3, the GDPR applies to entities or organisations established in the EU, notably entities that have an '**establishment**' in the EU or 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.	The CCPA and CPRA **apply** to entities that do business in the state of California. While not expressly defined within the CCPA, this could include: (i) having registered to do business with the Secretary of State; (ii) being subject to court jurisdiction; or (iii) active engagement with any transaction for financial gain or profit.

Differences

In relation to **extraterritorial scope**, the GDPR applies to the processing activities of data controllers and data processors that **do not have any presence in the EU**, where processing activities are related to the **offering of goods, or services to individuals in the EU, or to the monitoring of the behaviour of individuals in the EU**.	The CCPA and CPRA are **limited solely to California residents and entities doing business in the state** of California, while activities that occur wholly outside of California fall outside of the purview of the CCPA and CPRA.

1.3. Material scope

Fairly consistent

As it pertains to the material scope, the CCPA and CPRA generally apply to the same information and categories of information as with the GDPR. While the GDPR applies to activities involving the processing of personal data by either automated or non-automated means where the data in question is part of a filing system, the CCPA/CPRA do not delineate in the same way. Instead, the CCPA/CPRA apply with respect to obligations around 'collecting', 'selling', or 'sharing' of personal information.

GDPR	California Privacy Laws
Articles 2-4, 9, 26 Recitals 15-21, 26	Sections 1798.105, 1798.140, and 1798.145 of the CCPA Section 14 of the CPRA

Similarities

The GDPR defines '**personal data**' as 'any information' that directly or indirectly relates to an identified or identifiable individual. The GDPR does not apply to the personal data of deceased persons.

The CCPA and CPRA define '**personal information**' as anything that could be linked, directly or indirectly, with a particular consumer or household.

The GDPR defines **special categories of personal data** as 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**. The GDPR also provides specific requirements for its processing.

The CCPA, as amended by the CPRA, includes special categories of personal information, '**sensitive personal information**'. This includes **social security information, drivers' licenses, login information, credit card number, precise geolocation, racial or ethnic origin, the contents of email and text, as well as genetic data**.

The GDPR **excludes** from its application the 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.'

The CCPA **applies** to businesses that are collecting information and operating **for profit**. As such, non-profit entities generally would be exempt from the CCPA.

The GDPR **excludes** from its application data processing in the context of **law enforcement or national security**.

The CCPA and CPRA **permit** businesses to perform activities to comply with laws, **law enforcement** and civil, criminal, or regulatory actions.

The GDPR provides requirements for specific processing situations including processing for **journalistic purposes and academic, artistic or literary expression**.

The CCPA and CPRA provide **exceptions** for processing related to **public or peer-reviewed scientific, historical, or statistical research** in the public interests.

The GDPR excludes **anonymous data** from its application, which is defined as information that does not relate to an identified or identifiable natural person or to

The CCPA and CPRA exclude **anonymised** data, specifically any personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.

Similarities (cont'd)

personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.

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 and CPRA **apply** to the collection and use of personal data, and though 'processing' is not expressly defined, the CCPA and CPRA pertain to many similar activities.

Differences

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.'

The CCPA/CPRA are **not limited in their applicability** to information collected electronically or over the internet, but apply to the collection and sale of all personal information collected by a business from consumers.

2. Key definitions

Fairly consistent

2.1. Personal data

The GDPR, CCPA and CPRA refer to 'personal data' and 'personal information' respectively, both of which are broadly defined.

Under the CCPA and CPRA, the definition of 'personal information' provides practical examples of what information that relates to an identified or identifiable person could mean. For example, the definition refers to information relating to both individuals and households. The GDPR on the other hand only explicitly refers to individuals to whom its requirements will relate provided they are identifiable, in accordance with the definition of 'personal data'.

Moreover, while the GDPR expressly defines sensitive data as special categories of data, 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. Both the GDPR and the CCPA/CPRA provide for increased requirements when businesses process such categories of data.

However, one notable difference is that while the GDPR protects data related to health to a higher degree as 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	California Privacy Laws
Articles 4(1), 9 Recitals 26-30	Section 1798.140(b), (o) and (v)(2) of the CCPA Section 14 of the CPRA

Similarities

The GDPR defines '**personal data**' 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 CCPA and CPRA define '**personal information**' 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. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is **reasonably** capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household:

- identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, internet protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers;
- any personal information described in Section 1798.80(e) of the CCPA;
- characteristics of protected classifications under California or federal law;
- 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, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an internet website, application, or advertisement;
- geolocation data;
- audio, electronic, visual, thermal, olfactory, or similar information;
- professional or employment-related information;
- education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act of 1974; 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, behaviour, attitudes, intelligence, abilities, and aptitudes.

'Personal information' under the CCPA does not include consumer information that is de-identified or aggregate consumer information.

The CPRA will include in this definition of 'personal information', sensitive personal information as well.

The GDPR defines **special categories of personal data** as data revealing a data subject's 'racial or ethnic origin, political opinions, religious or philosophical beliefs, 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.

The CPRA defines '**sensitive personal information**' as:

- personal information that reveals:
  - a consumer's social security, driver's license, state identification card, or passport number;
  - a consumer's account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account;
  - a consumer's precise geolocation;
  - a consumer's racial or ethnic origin, religious or philosophical beliefs, or union membership;
  - the contents of a consumer's mall, email and text messages, unless the business is the intended recipient of the communication; and
  - a consumer's genetic data;

Similarities (cont'd)

GDPR	California Privacy Laws
	• the processing of: ◦ biometric information for the purpose of uniquely identifying a consumer; ◦ genetic data; ◦ personal information collected and analysed concerning a consumer's health; or ◦ personal information collected and analysed concerning a consumer's sex life or sexual orientation. The CCPA, with some amendments from the CPRA, will define '**biometric information**' as an individual's physiological, biological or behavioural characteristics, including information pertaining to an individual's deoxyribonucleic acid ('DNA'), that is used or intended to 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.
The GDPR specifies that **online identifiers** may be considered as personal data, such as IP addresses, cookie identifiers, and radio frequency identification tags.	Personal information includes '**identifiers** such as a real name, alias, postal address, unique personal identifier, online identifier, internet protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers'.
The GDPR **does not** apply to 'anonymised' data, where the data can no longer be used to identify the data subject.	The CCPA and CPRA **exclude anonymised data**, specifically any personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.

Differences

GDPR	California Privacy Laws
The GDPR **does not** contain a similar provision.	Sensitive personal information that is **publicly available** is not considered 'sensitive personal information' or 'personal information'. Personal information also does not include deidentified or aggregate consumer information. Under the CPRA, 'personal information' **does not include** publicly available information or lawfully obtained, truthful information that is a matter of public concern. For these purposes, '**publicly available**' means information that

Differences (cont'd)

GDPR	California Privacy Laws
	is lawfully made available from federal, state, or local government records, or if any conditions associated with such information that a business has a reasonable basis to believe is lawfully made available to the general public by the consumer or from widely distributed media, or by the consumer; or information made available by a person to whom the consumer has disclosed the information if the consumer has not restricted the information to a specific audience.

2.2. Pseudonymisation

Fairly consistent

Under the GDPR and the CCPA/CPRA, the definitions of pseudonymisation are fairly similar, defining it as the processing of personal data or information in a way that the data or information cannot be attributed to an identified or identifiable person without using additional information, as well as requiring that any such additional information is kept separately and secured.

GDPR	California Privacy Laws
Articles 4(5), 11 Recitals 26, 29	Sections 1798.140(r), and 1798.145(k) of the CCPA Section 14 of the CPRA

Similarities

The GDPR defines **pseudonymised data** as 'the processing of personal data in such a manner that the personal data that 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.'

The CCPA defines **pseudonymisation** as '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'.

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 their identification in order for the controller to be able to comply with **requests for the rights of the data subject**.

The CCPA **provides** that nothing should 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.

2.3. Controllers and processors

Fairly consistent

The term 'businesses' under the CCPA/CPRA bears similarity with the GDPR's 'data controllers', where both are responsible for complying with specific obligations with respect to their processing of data. However, one difference is that the GDPR places more responsibility and detailed obligations on 'data processors' which process personal data on behalf of data controllers, compared to the comparable 'service providers' under the CCPA/CPRA.

With respect to having contracts in place to regulate this relationship between data controller and data processors or businesses and service providers, the GDPR provides for detailed contract requirements to be in place. Similarly, the CCPA/CPRA also requires that a written contract be in place to regulate the disclosure of personal information to service providers.

GDPR	California Privacy Laws
Articles 4, 17, 28, 30, 32, 33, 35, 37, 38 Recitals 64, 90, 93	Sections 1798.105, 1798.140, 1798.145, 1798.155 of the CCPA Sections 4, 6, 14, 21 of the CPRA

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

Data controllers must comply with the **purpose limitation and accuracy principles, and rectify** a data subject's

A **business** is defined as a for-profit entity that collects consumers' personal information or on the behalf of which that information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information, that does business in the State of California, and that meets certain criteria.

Under the CCPA, a **service provider** is defined as a for profit legal entity that processes information on behalf of a business and to which the business discloses a consumer's personal information for a business purpose pursuant to a written contract, provided that the contract prohibits 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 for the business.

The CPRA expands this definition with some amendments, including expanding the prohibitions around the service provider's use of the data, as well as expanded obligations to notify the business about certain processing activities.

Furthermore, the CPRA includes new definitions for '**contactor**' and '**third party**'.

The CPRA will amend the CCPA to require businesses to comply with consumers' requests to **rectify their**

Similarities (cont'd)

GDPR	California Privacy Laws
personal data if it is **inaccurate** or **incomplete**.	**personal information**, and are required to **rectify any inaccurate or incomplete** information.
Data controllers must implement **technical and organisational security measures**, and notify supervisory authorities of **data breaches**.	Under the CPRA, a business that collects a consumer's personal information shall implement **reasonable security procedures and practices** appropriate to the nature of the personal information to protect the personal information.
The GDPR stipulates that data controllers and data processors keep **records of processing activities** and provides an exception from this obligation for small organisations.	Under the CPRA, the newly established CPPA will issue regulations specifying **record keeping requirements** for businesses.
The GDPR provides that where processing is to be carried out on behalf of a controller, the **controller shall use only data processors providing sufficient guarantees to implement appropriate technical and organisational measures** in such a manner that processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subject. In addition, the data processor shall not engage another data processor without prior specific or general written **authorisation** of the controller.	Businesses also have certain **disclosure requirements** when collecting or selling personal data, and are required to disclose consumer's personal information for a business purpose pursuant to a written contract. The CPRA stipulates that the **business shall enter into an agreement with a service provider** that obligates it to comply with applicable obligations under the CPRA and to provide the same level of privacy protection as is required by the law. Moreover, the agreement shall grant the business rights to take reasonable and appropriate steps to help to ensure that the service provider uses the personal information transferred in a manner consistent with the business's obligations under the CPRA. In addition, the service provider shall not engage another subprocessor without notifying the business of such engagement, and the engagement shall be pursuant to a written contract binding the other person to observe all the requirements set forth.

Differences

GDPR	California Privacy Laws
The GDPR provides that a data controller or data processors conduct **Data Protection Impact Assessments ('DPIAs')** in certain circumstances.	Although the CCPA and CPRA **do not** explicitly refer to 'DPIAs', the CPRA allows regulation on the matter to require businesses to **conduct risk assessments** in certain circumstances on an annual basis.

Differences (cont'd)

GDPR	California Privacy Laws
Data controllers based outside the EU and involved in certain forms of processing, with exceptions based on the scale of processing and type of data, are obliged to **designate a representative based within the EU** in writing.	The CCPA and CPRA **do not** include mandatory provisions on designating a representative based in California for a business based outside of the State.
The GDPR provides for the designation of a **data protection officer ('DPO')** by data controllers or data processors and defines the role of a DPO (see section 4.4.).	The CCPA and CPRA **do not** specify an obligation to appoint a DPO.

2.4. Children

Fairly inconsistent

While both the GDPR and the CCPA/CPRA have rules specific to the protection of children, their provisions differ in scope. The GDPR contains provisions which require special protection for children, but also provides specific provisions for protecting children's personal data with respect to processing for the provision of information society services. Contrastingly, while the CCPA also creates a special rule for children with regard to the selling and sharing of their data, it does not limit this rule to information society services. However, it should be noted that being a part of the US, the CCPA has some overlap with the federal Children's Online Privacy Protection Act of 1998 ('COPPA').

Regarding the age of consent of children, the GDPR parental or guardian consent on behalf of children under the age of 16 is required, with Member States being permitted to lower this age requirement to 13. Contrastingly, the CCPA and CPRA introduce an opt-in requirement for the selling and sharing of personal information of minors under 16 years old, while parents or legal guardians are required to opt-in for minors at least 13 and under 16.

Additionally, while the GDPR allows for other lawful grounds other than consent for the processing of children's data, the CCPA provides that the sale of personal information is only permitted on the basis of consent.

GDPR	California Privacy Laws
Articles 6, 8, 12, 40, 57 Recitals 38, 58, 75	Section 1798.120(c) of the CCPA Section 9 of the CPRA

Similarities

GDPR	California Privacy Laws
The GDPR **does not** define 'child' nor 'children.'	The CCPA and CPRA **do not** define 'child' nor 'children'. However, the CCPA provides for opt-in rights for minors under the age of 16.
Where the processing is based on consent, the 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 **lower this age limit to 13**.	Businesses must have opt-in consent to sell or share the personal information of consumers under the **age of 16** if they have actual knowledge that a consumer is under the age of 16. For consumers at least 13 years of age and less than 16 years of age, the child's parent or guardian must affirmatively authorise the sale or sharing of the child's personal information. A business that willfully disregards the consumer's age shall be deemed to have had actual knowledge of the consumer's age.

Differences

GDPR	California Privacy Laws
The GDPR considers children as '**vulnerable natural persons**' that merit specific protection with regard to their personal data. In particular, specific protection should be given when children's personal data is used for **marketing or collected for information society services** offered directly to a child.	The CCPA/CPRA **do not** contain a similar provision.
When any information is addressed specifically to a child,	The CCPA/CPRA **do not** contain a similar provision.

GDPR	California Privacy Laws

Differences

GDPR	California Privacy Laws
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 GPDR provides that data controllers are required to make reasonable efforts to **verify** that **consent** is given or authorised by a parent or guardian.	The CCPA/CPRA **do not** contain a similar provision.
The GDPR **does not** explicitly outline an exception for actual knowledge of a child's age.	The CCPA provides for an **exception** for businesses that did not have **actual knowledge of a child's age**.

2.5. Research

Under the GDPR, specific provisions regulate the processing of personal data for 'historical or scientific research', and for processing for 'statistical purposes'. Moreover, exceptions in this regard are also provided for under the GDPR, which include specific requirements regarding the lawful basis for processing, as well as a specific exception to the right of erasure. Member States are also permitted to implement derogations from the rights of the data subject where personal data is processed for scientific or historical research purposes.

The CCPA and CPRA also define research broadly, outlining that the processing of consumer data obtained in the course of providing a service can be further processed for research purposes, as this may be considered compatible with the initial business purpose for the processing of the data. However, and unlike the GDPR, the CCPA/CPRA do not have or provide for an overarching principle of purpose limitation that would limit the purposes for which a business can use personal information.

The GDPR also requires that controllers have in place technical and organisational measures for the processing of personal data for research purposes. Similarly, the CCPA also requires that safeguards be put in place, but provides a detailed list of such measures.

Another difference between the laws is that the CCPA excludes clinical trials from its scope of application, while the GDPR does not.

GDPR	California Privacy Laws
Articles 5(1)(b), 9(2)(j), 14(5), 17(3), 21(6), 89 Recitals 33, 159-161	Sections 1798.105, 1798.140, 1798.145 of the CCPA Sections 5 and 14 of the CPRA

Similarities

According to the GDPR, **the processing of sensitive data is not prohibited when 'necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes**, 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.'

According to the CCPA, **processing is not prohibited when necessary for research**. '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.

The CPRA will introduce some amendments to this definition, defining 'research' as scientific analysis, systematic study and observation, including basic research or applied research that is designed to develop or contribute to public or scientific knowledge and that adheres or otherwise conforms to all other applicable ethics and privacy laws, including but not limited to studies conducted in the public interest in the area of public health.

The data subject has the right to object to the processing of personal data for research purposes **unless such research purposes are for reasons of public interest.**

The CCPA provides that 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.

GDPR	California Privacy Laws

Similarities (cont'd)

The GDPR provides that 'further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), **not be considered to be incompatible with the initial purposes**'.

The CCPA also imposes safeguards for research conducted on consumer information collected initially for other purposes. For example, the CCPA requires that:

- the personal information be subsequently **pseudonymised and deidentified**;
- should be made subject to **technical safeguards** that prohibit reidentification of the consumer to whom the information may pertain, other than as needed to support the research;
- 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 f**or research purposes that are compatible** with the context in which the personal information was collected; and
- should be subject to **additional security controls** that allow access to this information on an only need-to-know basis.

Under the GDPR, where personal data are processed for research purposes, it is possible for **Member States to derogate from some data subjects' rights**, including the right to access, the right to rectification, the right to object and the right to restrict processing, insofar as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such **derogations** are necessary for the fulfilment of those purposes.

The CCPA provides that a business or a service provider shall not be required to comply with a consumer's request to delete their personal information if it is necessary to maintain this information in order to engage in **public or peer-reviewed scientific, historical, or statistical research in the public interest**, when the business' deletion of the information is likely to render impossible or seriously impair the achievement of such research, and if the consumer has provided informed consent.

Differences

Under the GDPR, the processing of personal data for research purposes is subject to **specific rules** (e.g. with regard to the purpose limitation principle, right to erasure, data minimisation and anonymisation etc.).

The CCPA/CPRA **do not** outline specific riles for the processing of personal data for research purposes. Regarding the understanding of 'business purpose', undertaking internal research for technological development and demonstration is considered a business purpose.

The GDPR clarifies that the processing of personal data for **scientific research** purposes should be interpreted 'in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research.'

The CCPA **excludes clinical trials** from its scope of application. The CPRA expands on this and provides that this applies provided that such information is not sold or shared in a manner not permitted by the CCPA, and if it is inconsistent, that participants be informed of such use and provide consent.

3. Legal basis

To compare the GDPR with the CCPA and CPRA, it is important to note that processing under the GDPR is explicitly defined to be operation(s) performed on personal data or sets of personal data, including 'collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure, dissemination, restriction or destruction'. Whereas the CCPA and CPRA do not explicitly reference collection.

Additionally, and under the GDPR, processing of personal data is only considered to be lawful when one of the six legal grounds for processing under Article 6 are fulfilled, namely consent, the performance of a contract, complying with a legal obligation, to protect the data subject's vital interests, for the public interest, and for the legitimate interests pursued by the controller or by a third party. Contrastingly, the CCPA/CPRA do not outline a set list of grounds as legal bases for the processing of personal data, but provides for data subjects' right to opt-out or request the erasure of their data from processing through to collection, sale, or disclosure of their personal data.

GDPR	California Privacy Laws
Articles 4-10 Recitals 39-48	Sections 1798.100, 1798.105, 1798.121(d), 1798.140(h) and (q), and 1798.145(e) and (f) of the CCPA Sections 4, 5, 10, 14, and 15 of the CPRA

Similarities

The GDPR states that data controllers can only process personal data when there is a legal ground for it. The legal grounds are:

- **consent**;
- when processing is necessary for 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;
- compliance with **legal obligations** to which the data controller is subject;
- to protect the **vital interest** of the data subject or of another natural person;
- performance carried out in the **public interest** or in the official authority vested in the data controller; or
- 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).

The CCPA, as amended by the CPRA, permits businesses subject to the CCPA and CPRA to process personal data quite broadly. The legal grounds are, among others:

- **consent**;
- when processing is necessary for a **business purpose** pursuant to the initial notice or reason for collection;
- compliance with **legal obligations** that the business is subject to;
- engaging in public or peer reviewed **scientific, historical, or statistical interest**; and
- exercise or defence of **legal claims**.

There are specific **legal grounds for processing special categories of data**, such as explicit consent.

Regarding **special categories of data**, specific **notices are required** and there are restrictions on processing the information depending on its use.

Similarities (cont'd)

The GDPR recognises **consent** as a legal basis to process personal data and includes **specific information** on how consent must be obtained and can be withdrawn.

The GDPR defines consent as 'any **freely given, specific, informed and unambiguous indication** of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.'

The CCPA and CPRA recognise **consent** as a legal basis. Specific information regarding consent is also listed, including an explicit prohibition on dark patterns.

The CCPA and CPRA define consent as 'any **freely given, specific, informed, and unambiguous indication** of the consumer's wishes'.

Differences

Under the GDPR, consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a **written statement, including by electronic means, or an oral statement**.

Consent is not explicitly required to process information in the same way that processing is defined under the GDPR. However, **notice** is required **prior to**, **or at the point of, collection.**

The GDPR **does not** contain similar provisions with respect to such legal bases for processing personal data.

The CCPA, as amended by the CPRA, permits businesses subject to the CCPA and CPRA to process personal data **broadly**, and includes legal grounds such as:

- when processing is necessary for a **business purpose** pursuant to the initial notice or reason for collection; or
- **debugging or identifying and repairing** errors.

4. Controller and processor obligations

4.1. Data transfers

Fairly inconsistent

The concept of data transfers under the GDPR is substantially different from the CCPA and CPRA, where transferring under the CCPA/CPRA falls within the definition of sharing personal information. Nonetheless, the CCPA and CPRA do find consistency with the GDPR in some regards, namely those related to specific requirements for third party entities, particularly with the CPRA's expansion of contracting requirements to include third parties and contractors.

GDPR	California Privacy Laws
Articles 44-50 Recitals 101, 112	Sections 1798.105, 1798.121, 1798.130, 1798.140, 1798.145 of the CCPA Sections 5, 10, 12, 14, and 15 of the CPRA

Similarities

The GDPR allows personal data to be transferred to a third country or international organisation that has an **adequate level of protection** as determined by the EU Commission.

The CCPA/CPRA permits the transfer of information in the event that the recipient entity is obligated to provide the **same level of privacy protection** required under the Statute.

One of the following **legal grounds** can be applied to the transfer of personal data abroad:

- prior **consent;**
- when a data subject has explicitly **consented** to the proposed transfer and acknowledged the possible risks of such transfer due to inadequate safeguards;
- when the transfer is necessary for the performance or conclusion of a **contract**;
- when the transfer is necessary for important **public interest** reasons;
- when the transfer is necessary for the establishment, exercise, or defence of a **legal** claim; and
- when the transfer is necessary to protect the **vital interests** of a data subject or other persons.

The following legal grounds, among others, are applicable to the transfer of personal data, though vary depending on the situation:

- **consent**;
- compliance with **legal obligations** that the business is subject to;
- engaging in public or peer reviewed scientific, historical, or statistical interest; and
- exercise or defence of **legal claims**.

Differences

The GDPR specifies that a cross-border transfer is allowed based on **international agreements** for judicial cooperation.

The CCPA/CPRA **do not** address cross-border transfers based on international agreements for judicial cooperation.

GDPR	California Privacy Laws

Differences (cont'd)

In the absence of a decision on adequate level of protection, a transfer is permitted when **the data controller or data processor provides appropriate safeguards** with effective legal remedies that ensure the data subjects' rights as prescribed under the GDPR. Appropriate safeguards include:

- **binding corporate rules** with specific requirements (e.g. a legal basis for processing, a retention period, complaint procedures, etc.);
- **standard data protection clauses** adopted by the EU Commission or by a supervisory authority;
- an **approved code of conduct**; or
- an **approved certification mechanism**.

The CCPA/CPRA **do not** explicitly address transfer mechanisms. Instead, transfers of personal data to third parties are conditioned on the third party providing the same level of protection of the consumer's rights.

The grounds for a **cross-border transfer includes the transfer being made from a register** which, according to the Union or a Member States' law, is intended to provide information to the public, and which is open to consultation either by the public in general or by any person who can demonstrate a **legitimate interest**, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case.

The CCPA/CPRA **do not** contain a similar provision.

The GDPR **does not** provide similar grounds as a legal basis for the transfer of personal data.

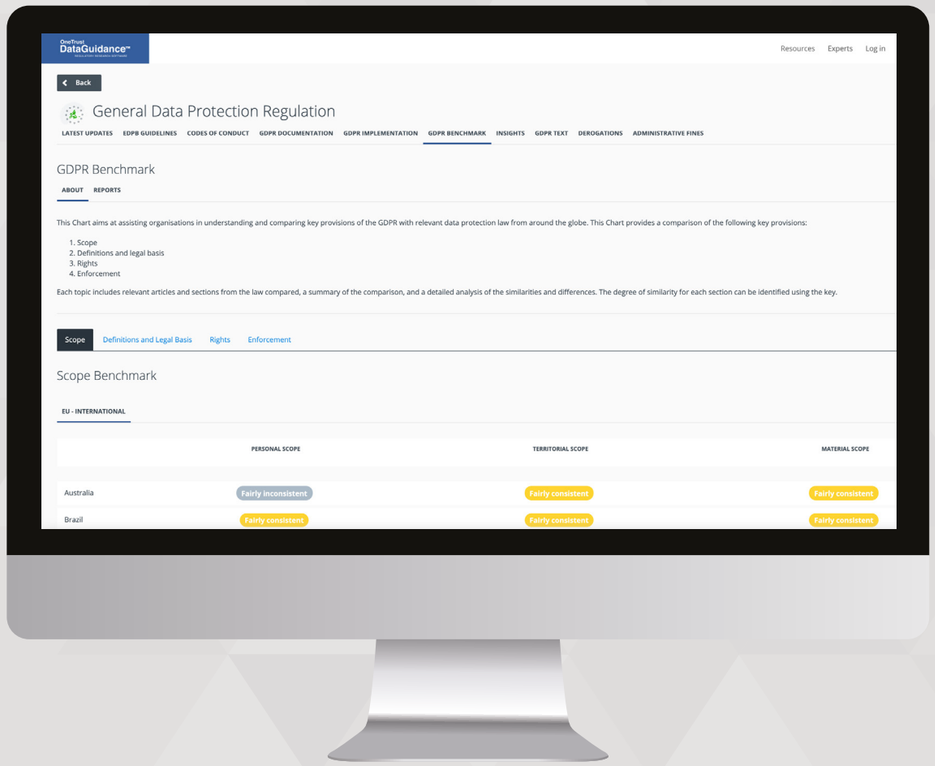
The transfer of personal data can be justified through certain legal grounds, among others, although these may vary depending on the situation:

- when processing is necessary for a **business purpose** pursuant to the initial notice or reason for collection;
- **debugging or identifying and repairing** errors; and
- any **internal lawful use** in the same context in which the consumer provided the information.

Global Regulatory Research Software

40 In-House Legal Researchers, 500 Lawyers Across 300 Jurisdictions

Monitor regulatory developments, mitigate risk, and achieve global compliance



OneTrust
DataGuidance™
REGULATORY RESEARCH SOFTWARE

Build a global privacy program by comparing key legal frameworks against the GDPR

CCPA | Russia | Thailand | Brazil | Japan | China
and 20+ other global laws & frameworks

Understand and compare key provisions of the GDPR with relivant data protection laws from around the globe

The GDPR Benchmarking tool provides comparison of the various pieces of legislation on the following key provisions

- Scope
- Rights
- Definitions and legal basis
- Enforcement

- Employ topic specific guidance to develop your compliance activities
- Monitor news and access written opinion pieces on the most recent developments

Start your free trial at
www.dataguidance.com

4.2. Data processing records

Fairly inconsistent

Record maintenance is needed to cover any data which is collected, and the CCPA/CPRA require maintaining records for satisfying consumer requests, and that notices must be provided at the outset and prior to the collection of any data. Thus, although there are some inconsistencies with the GDPR around requirements to keep records, the laws are similar in the list of information that needs to be provided at the outset.

GDPR	California Privacy Laws
Article 30 Recital 82	Sections 1798.105, 1798.121, 1798.130, 1798.140, 1798.145 of the CCPA Sections 5, 10, 12, 14, and 15 of the CPRA Sections 999.312, 999.313, and 999.317 of the CCPA Regulations

Similarities

Data controllers and data processors have an obligation to **maintain a record** of processing activities under their responsibility.

Entities subject to the CCPA are required to **maintain records** of verifications of requests and to provide a general guideline of what information is collected.

The obligations in relation to data processing records are also imposed on the **representatives of data controllers.**

The business collecting and then disclosing or selling personal information is required to specify limitations on the information sold and **require that the recipients have in place systems** whereby they can fulfil consumer requests.

The **processing of information recorded by a data controller** shall be in writing or electronic form.

The CCPA requires that **records of consumer requests are kept by the business satisfying such requests**. However, neither the CCPA or CPRA explicitly address the form of the requests.

Differences

The GDPR **prescribes a list of information that a data controller** must record:

- the name and contact details of the **data controller;**
- the **purposes of the processing**;
- a description of the categories of **personal data**;
- the categories of recipients to whom the personal data will be **disclosed**;
- the **estimated period for erasure** of the categories of data; and
- a general description of the technical and organisational **security measures** that have been adopted.

The CCPA and CPRA require that the entity **provides the following at the outset**, prior to collection:

- contact information for the business to exercise rights, specifically two different methods, including a toll-free phone number;
- the categories of personal information collected;
- the purposes of the collection and processing; and
- specification whether the information is sold or disclosed by the business.

The GDPR **prescribes a list of information that a data controller** must record **international transfers** of personal data, with the

The CCPA/CPRA **do not** contain a similar provision.

GDPR	California Privacy Laws

Differences (cont'd)

identification of third countries or international organisations, and the documentation of adopted suitable safeguards.

The requirements around data processing records shall not apply to **an organisation with less than 250 employees**, unless the processing:

- is likely to result in a risk to the rights and freedoms of data subjects;
- is not occasional; or
- includes special categories of data in Article 9(1) (e.g. religious beliefs, ethnic origin, etc.) or is personal data relating to criminal convictions and offences in Article 10.

The CCPA and CPRA **do not set a minimum** employee number in order for businesses to be subjected to their provisions.

The GDPR **does not** provide general requirements for registering with a supervisory authority.

The CCPA/CPRA **do not** contain a similar provision.

4.3. Data protection impact assessment

Under the GDPR a DPIA is required and should contain a systematic description of the processing operations, an assessment of necessity and proportionality, and an assessment of the risks and freedom of data subjects, in addition to measures to address those risks. While the CCPA and CPRA do not explicitly refer to DPIAs the CPRA does introduce a provision outlining that the California Attorney General ('AG') has the authority to adopt regulations requiring businesses whose processing of consumers' personal information presents a significant risk to consumers' privacy or security, to submit on a regular basis a risk assessment with respect to their processing of personal information.

GDPR	California Privacy Laws
Article 35, 36 Recitals 75, 84, 89-93	Section 1798.100 of the CCPA Section 21 of the CPRA

Similarities

GDPR	California Privacy Laws
Not applicable.	Not applicable.

Differences

GDPR	California Privacy Laws
Under the GDPR, a **DPIA must be conducted** under specific circumstances.	The CCPA and CPRA do not explicitly refer to 'DPIAs'. However, it is contemplated that there are **annual audits** in cases where businesses whose processing of personal information presents risks to consumers, in addition to risk assessments. However, certain concepts, like proportionality and necessity, remain as concepts as it pertains to collection at the outset. This will change under the CPRA, which requires the AG to solicit broad public participation and adopt regulations on, among other things, requiring businesses whose processing of consumers' personal information presents significant risk to consumers' privacy or security, to: (a) perform a cybersecurity audit on an annual basis; and (b) submit to the CPPA on a regular basis a **risk assessment** with respect to their processing of personal information.
A data controller is required to, **where necessary**, carry out a review to assess whether the processing of personal data is in accordance with the DPIA, **particularly when there is a change** in risks to processing operations.	The CCPA **does not** contain a similar provision, although the CPRA will introduce certain requirements for risk assessments as detailed above.
The GDPR provides that a DPIA must be conducted if a data controller utilises **new technologies** to process personal data.	The CCPA **does not** contain a similar provision, although the CPRA will introduce certain requirements for risk assessments as detailed above.

GDPR	California Privacy Laws

Differences (cont'd)

GDPR	California Privacy Laws
The GDPR provides that a DPIA must be conducted **under the following circumstances**: • the processing may result in a high risk to the rights and freedoms of an individual; • when a systematic and extensive evaluation of personal aspects relating to natural persons is involved, which is based on automated processing or profiling; • there is processing on a large scale of special categories of data; and • there is systematic monitoring of a publicly accessible area on a large scale.	The CCPA **does not** contain a similar provision, although the CPRA will introduce certain requirements for risk assessments as detailed above.
The assessment **must contain at least** the following: • a systematic description of the envisaged processing; • operations and legitimate purposes of the processing; • the necessity and proportionality of the operations in relation to the purposes; and • the risks to the rights and freedoms of data subjects.	The CCPA **does not** contain a similar provision, although the CPRA will introduce certain requirements for risk assessments as detailed above.
A data controller **must consult** the supervisory authority prior to any processing that would result in a high risk in the absence of risk mitigation measures as indicated by the DPIA.	The CCPA **does not** contain a similar provision, although the CPRA will introduce certain requirements for risk assessments as detailed above.

4.4. Data protection officer appointment

Unlike the GDPR, the concept of a DPO is not required specifically within the CCPA and CPRA, though there are requirements regarding the training of those parties handling consumer requests under the CCPA and CPRA. As a result, it should be noted that a DPO-like role may be necessary to satisfy the CCPA and CPRA's requirements regarding having trained individuals responsible for handling consumer inquiries.

GDPR Articles 13 - 14, 37-39 Recital 97	California Privacy Laws Section 999.317 of the CCPA Regulations

Similarities

GDPR	California Privacy Laws
Not applicable.	Not applicable.

Differences

GDPR	California Privacy Laws
Under the GDPR, data controllers and data processors, including their representatives, are required to **appoint** a DPO in certain circumstances.	The CCPA and CPRA **do not** include a requirement for businesses to appoint a DPO.
The data controller and the data processor shall designate a DPO in any case where: • the processing is **carried out by a public authority or body**, except for courts acting in their judicial capacity; • the core activities of a data controller or data process or consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require **regular and systematic monitoring** of data subjects on a large scale; or • the core activities of the controller or the processor relate to a large scale of **special categories of personal data** (e.g. religious beliefs, ethnic origin, data required for the establishment, exercise, or defence of legal claims etc.)	The CCPA/CPRA **do not** contain a similar provision.
A group may appoint a **single DPO** who must be easily contactable by each establishment.	The CCPA/CPRA **do not** contain a similar provision.
The DPO shall perform a list of tasks including: • **to inform and advise** the controller or the data processor and the employees who carry out processing of their obligations pursuant to the GDPR and to other Union or Member State data protection provisions;	The CCPA/CPRA **do not** contain a similar provision.

GDPR	California Privacy Laws

Differences (cont'd)

GDPR	California Privacy Laws
• **to monitor** compliance with the GDPR with other Union or Member State data protection provisions and with the policies of the data controller or data processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits; and • **to act as a contact point** the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.	
The DPO shall be designated on the basis of **professional qualities and expert knowledge** of data protection law and practices.	The CCPA and CPRA **do not** include a similar requirement. However, it is required that all individuals responsible for handling consumer inquiries regarding privacy practices or compliance with the CCPA and CPRA are informed of all the requirements in the CCPA and the CCPA Regulations thereunder.
The DPO can be a **staff member** of the data controller or data processor, or can perform tasks based on a **service contract**.	The CCPA/CPRA **do not** contain a similar provision.
Contact details of the DPO must be included in the privacy notice for data subjects, and they must be communicated to the supervisory authority.	The CCPA/CPRA **do not** contain a similar provision.
Data subjects **may contact** the DPO with regard to the processing of their personal data as well as the exercising of their rights.	The CCPA/CPRA **do not** contain a similar provision.
The DPO must be **provided with the resources necessary** to carry out his or her obligations under the GDPR.	The CCPA/CPRA **do not** contain a similar provision.
The GDPR recognises the **independence** of DPOs.	The CCPA/CPRA **do not** contain a similar provision.

4.5. Data security and data breaches

Fairly consistent

While the CCPA and CPRA do require businesses to adopt reasonable security measures, notices are covered under a separate provision under California law. While there are striking similarities between what is required under the GDPR and California's laws, California adopts a slightly less prescriptive approach to the requirements to the GDPR.

GDPR	California Privacy Laws
Article 5, 24, 32-34 Recitals 74-77, 83-88	Sections 1798.100 and 1798.150 (in conjunction with Section 1798.82 of the Cal. Civ. Code) Sections 4, 14 and 16 of the CPRA Sections 999.313, 999.317, 999.323, and 999.326 of the CCPA Regulations

Similarities

The GDPR recognises **integrity** and **confidentiality** as **fundamental principles** of protection by stating that personal data must be processed in a manner that ensures appropriate security of the personal data.

The CPRA recognises and provides a definition of '**security and integrity**'.

In addition, the CCPA and CPRA generally recognise privacy rights of consumers, providing various methods for them to exert control over their own information. As part of this, **verification measures** are implemented as part of consumer requests under the act.

The GDPR states that **data controllers and data processors are required to implement appropriate technical and organisational security measures** to ensure that the processing of personal data complies with the obligations of the GDPR.

The CCPA and CPRA require that **reasonable security measures** are enacted to ensure that information is adequately protected, including verification of consumer requests.

In the case of a personal data breach, the **data controller must notify the competent supervisory authority** of the breach, unless the personal data breach is unlikely to **result in a risk** to the individuals' rights and freedoms.

In the event of a data breach, the business is to **notify the AG** of the **breach** in the event that the notice needs to be submitted to over **500 California residents** as a result of a single breach.

The controller must **notify** the **data subject** of a data breach **without undue delay** if the data breach is likely to result in a **high risk** to the rights and freedoms of natural persons.

The **notice** of a data breach to affected **California residents** is to be in the **most expedient time possible** and **without unreasonable delay**, but may be delayed due to requests by law enforcement.

The GDPR **provides a list of information** that must be, at minimum, **included in the notification** of a personal data breach. For example, a notification must describe the nature of the breach, the approximate number of data subjects concerned, and the consequences of the breach.

California has specific requirements as to what needs to be **included within the data breach notification**, including, at minimum:

- what happened;
- what information was involved;

GDPR	California Privacy Laws

Similarities (cont'd)

- what the business is doing; and
- what the individual affected can do.

Differences

Under the GDPR, a personal data breach must be notified to the supervisory authority **without undue delay** and, where feasible, **no later than 72 hours** after having become aware of the breach.

Notice under California law is determined by the amount of affected persons. However, there is **no prescribed timeline** to notify the AG under California's data breach notification law.

Under the GDPR, the obligation of data controllers to notify data subjects when the data breach is likely to result in a high risk to the rights and freedoms of natural persons, is **exempted in certain circumstances** such as where:

- appropriate technical and organisational protective measures have been implemented;
- any subsequent measures have been taken in order to ensure that the risks are no longer likely to materialise; or
- it would involve is proportionate effort.

The CCPA/CPRA **do not** include similar provisions regarding exemptions.

The GDPR provides a **list** of **technical and organisational measures**, where appropriate, that data controllers and data processors may implement such as pseudonymisation, encryption and the ability to restore availability and access to personal data in a timely manner in the event of physical or technical incidents, to ensure integrity and confidentiality.

Specific obligations regarding security have not been implemented. Ultimately, as '**reasonable security**' can vary based on what information is collected, and what information needs to be disclosed, the measure of the security will vary and so, solid guidelines or methods to determine what is 'reasonable' is unavailable.

The GDPR states that **data processors must notify** the data controller without **undue delay** after becoming aware of the personal data breach.

The CCPA/CPRA **do not** contain a similar requirement, and notices are covered under a separate provision under California law, specifically under Section 1798.82 of Title 1.81. of Part 4 of Division 3 of the Cal. Civ. Code.

4.6. Accountability

While the CCPA and CPRA do not specifically reference 'accountability' as a 'fundamental principle', as is the case with the GDPR, they do determine that the business entities responsible for requesting and processing the information are responsible for ensuring third parties acting on their behalf follow the CCPA and CPRA.

GDPR	California Privacy Laws
Articles 5, 24-25, 35, 37 Recital 39	Sections 1798.100 and 1798.145 of the CCPA

Similarities

The GDPR recognises **accountability** as a fundamental principle of data protection. Article 5 states that 'the data controller shall be responsible and able to demonstrate compliance with, paragraph 1 [accountability].' In addition, the principles can be taken to apply to several other principles as mentioned in other sections of this report, including the appointment of a DPO, and DPIAs.

The CCPA and CPRA do not expressly recognise **accountability**, but do recognise that the primary entity collecting data is ultimately responsible for the obligations of following the CCPA and CPRA, including themselves and third parties acting on their behalf.

Differences

The GDPR **explicitly** recognises accountability as a fundamental principle.

There is **no explicit provision** regarding accountability.

5. Rights

5.1. Right to erasure

The right to erasure under the CCPA and CPRA is generally similar to that which is outlined under the GDPR, which should not be a major surprise as the inspiration for the provisions came from the general 'right to be forgotten' that emerged as part of the GDPR.

Nevertheless, there are still some differences between these laws, such as with timelines for complying with a data subject's request to exercise their data subject right. Additionally, the CCPA/CPRA provides for, among other things, the possibility of maintaining confidential records of deletion requests to prevent such information from being sold, for compliance with laws, or for other permissible purposes.

GDPR	California Privacy Laws
Articles 12, 17 Recitals 59, 65-66	Section 1798.105 of the CCPA Sections 3 and 5 of the CPRA Sections 1546 to 1546.4 of Chapter 3.6 of Title 12 of Part 2 of the California Penal Code ('the Penal Code')

Similarities

The GDPR provides for a **right to erasure** which applies to specific grounds, such as where consent of the data subject is withdrawn and there is no other legal ground for processing, or the personal data is no longer necessary for the purpose of which it was collected.

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

Data subjects **must be informed** that they have the right to request for their data to be deleted and are entitled to ask for their data to be erased.

If the data controller has made personal data public and is obliged to erase the personal data, the data controller, taking into account the available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers processing the personal data that the data subject has

The CCPA and CPRA both provide for a consumers' **right to delete personal information**. A consumer has the right to request that a business delete any personal information about the consumer which the business has collected from the consumer.

There is **no cost** to making a request to delete personal information. However, the request must be verified as coming from the consumer.

Consumers **must be informed** that they have a right to request deletion of their personal information.

A business that has shared any personal information with outside sources must **notify all service providers, contractors and third parties** to whom the business has sold or shared personal information, to delete the consumer's personal information, unless this proves impossible or involves disproportionate efforts.

GDPR	California Privacy Laws

Similarities (cont'd)

requested the erasure by such controllers of any links to, or copy or replication of, such personal data.	
Exceptions to the right of erasure provided by the GDPR include: • **freedom of expression** and freedom of information; • complying with **public interest purposes in the area of public health**; • establishment, exercise, or defence of **legal claims**; and • **complying with legal obligations** for a public interest purpose.	Exceptions to the right to deletion under both the CCPA and CPRA include the following scenarios: • where the personal information is required to **complete the transaction** for which the personal information was provided; • to **ensure security and integrity** to the extent the use of the consumer's personal information is reasonably necessary and proportionate for those purposes; • to **debug, identity, and repair errors**; • **exercising free speech**; • compliance with the California Electronic Communications Privacy Act under the Penal Code; • engage in **scientific research**; • for solely **internal uses** at a business; and • comply with a legal obligation.
A request can be made in **writing, orally, and through other means including electronic means** where appropriate.	A request can be made in **writing, orally, and through other means or electronic means** where appropriate.
A data controller must have in place mechanisms to ensure that **the request is made by the data subject** whose personal data is to be deleted.	The request must be a **verified consumer request**.

Differences

Data subject requests under this right must be replied to without 'undue delay and in any event within **one month** from the receipt of request.' The deadline can be extended by **two 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.	As with other consumer requests, a request for deletion must be responded to, and information deleted, within **45 days, with an additional 45-day extension** available, with notice to the consumer. Additionally, a business must acknowledge receipt of a request to delete within ten business days of receipts.
The GDPR **does not** contain a similar provision or requirements.	The business may maintain a **confidential record** of deletion requests solely for the purpose of **preventing** the personal information of a consumer who has submitted a deletion request from being **sold, for compliance with laws, or for other permissible purposes**.

GDPR | California Privacy Laws

Differences (cont'd)

The GDPR **does not** provide for a similar requirement.	A **service provider or contractor** must **cooperate** with the business in responding to a request for deletion, delete any such requested personal information, and **give notice** to any additional service provider, contractor, or third party to whom the service provider or contractor has shared the consumer's personal information of their obligation to delete the personal information as well.
The GDPR **does not** contain a similar provision or requirement.	A service provider or contractor **does not need to comply** with a deletion **request received directly from the consumer**, to the extent that the service provider or contractor received the personal **information directly from the business**. Rather, the request should be made directly to the business as opposed to the service provider or contractor.

5.2. Right to be informed

Fairly consistent

Unlike the GDPR, the CCPA/CPRA do not explicitly refer to a 'right to be informed'. However, California has implemented various required disclosures which collectively create a 'right to know'. This includes many of the same aspects contained within the GDPR, giving consumers similar rights regarding their information.

GDPR	California Privacy Laws
Articles 5-14, 47 Recitals 58-63	Sections 1798.100, 1798.110, and 1798.115 of the CCPA Sections 4 and 7 of the CPRA

Similarities

Data subjects have the right to receive information on the following, among other things, at the time of collection where data is collected from them: • the **identity and the contact details of the controller** or controller's representative; • the **contact details of the DPO**; • the **purposes of the processing** as well as the **legal basis for the processing**; • any **legitimate interests** pursued by the controller or by a third party, if applicable; • the **recipients or categories of recipients** of the personal data, if any; • where applicable, the fact that the controller intends to **transfer personal data to a third country** and related information; • the **period for which the personal data will be stored**, or if that is not possible, the criteria used to determine that period; • the **data subject's rights**; and • whether the provision of personal data is an **obligation**.	Consumers have the **right to know**, and businesses who collect personal information must inform consumers, at or before the time of collection, of the following information about the personal information: • the **categories of personal information** it has collected from consumers; • **under the CPRA**, a business must also **disclose categories of sensitive personal information** collected; • the **categories of sources** from which the personal information or sensitive personal information is collected; • the **business purpose** for such collection, sharing, or selling; • the **categories of third parties** to whom to personal information or sensitive personal information is disclosed to; • that a consumer has the r**ight to request the specific pieces of personal information** collected; and • the length of time that the business intends to retain each category of personal information and sensitive personal information.
Information should be provided to data subjects in an easily accessible form with clear and plain language, which can be in **writing and other means such as an electronic format**.	The responses must be in a **readily useable format** that allows the consumer to transmit the information to another entity without hindrance.
A data controller cannot collect and process personal data for **purposes other than the ones about which the data subjects were informed**, unless the data controller provides them with further information.	A business's collection, use, retention, and sharing of a consumer's personal information must be reasonably necessary and proportionate to achieve the **purposes for which the personal information was collected or processed**, and not for undisclosed business purposes.
The GDPR provides specific information that must be given to data subjects when their personal	The CCPA and CPRA require businesses to provide **categories of sources** from which personal information is collected.

GDPR	California Privacy Laws

Similarities (cont'd)

data has been **collected from a third party**, which includes the sources from which the data was collected.	
Information relating to personal data processing (e.g. the purpose of the processing, the rights of data subjects, etc.) must be provided to data subjects by the data controller **at the time when personal data is obtained**.	The CCPA and CPRA require transparency at the **time of collection** as to specific information regarding a consumer's personal information – including what will be collected, why, and with whom the personal information will be sold, shared, or disclosed.

Differences

Data subjects must be informed of the existence of **automated decision-making, including profiling**, at the time when personal data is obtained.	The CCPA/CPRA **do not** contain a similar requirement.
Information can be provided to data subjects **orally**, in addition to in writing form or electronic means.	The CCPA and CPRA **only** contemplate providing responses to consumer requests in a written or electronic format, not orally.
The GDPR **provides examples** of circumstances, which can be considered as 'legitimate interest.'	The CCPA/CPRA **do not** contain a similar provision.
Data subjects must be informed of the **possible consequences** of a failure to provide personal data whether in complying with statutory or contractual requirements, or a requirement necessary to enter into a contract.	The CCPA/CPRA **do not** contain a similar provision.
A data controller must **inform** data subjects of the existence or absence of an adequacy decision, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference the **appropriate or suitable safeguards** and the means by which to obtain a copy of them or where they have been made available.	The CCPA/CPRA **do not** contain a similar provision.
In the case of indirect collection, a data controller must provide information relating to such collection to data subjects 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 when personal data is first disclosed to the recipient**.	The CCPA/CPRA **do not** contain a similar provision, but requires, in the context of disclosure obligations for collecting and selling personal information, that businesses disclose, among other things, the **categories of sources** from which information is collected.

5.3. Right to object

Fairly consistent

Similar to the GDPR's broader right to object to any kind of processing of personal data, the CCPA and CPRA present a comparable right, namely allowing consumers to opt-out of the sale of their personal information. The CPRA would slightly extend this by requiring businesses to comply with a consumer's direction that a business limit use of sensitive personal information to that use which is necessary to perform the services or provide the goods reasonably expected by an average consumer.

GDPR	California Privacy Laws
Articles 7, 12, 18, 21	Sections 1798.120 and 1798.121 of the CCPA Sections 9 and 10 of the CPRA

Similarities

GDPR	California Privacy Laws
Data subjects shall have the right to **withdraw** their consent to the processing of their personal data **at any time**.	A consumer shall have the right to direct a business **not to sell or share** the personal information with a third party.
The data subject has the right to be **informed** about the right to object.	A **consumer must be provided explicit notice** that the consumer has the right to opt-out of the sale or sharing of their personal information.
Upon the **receipt of an objection** request, a data controller shall **no longer process** the personal data unless an exception applies.	Upon **receiving direction from a consumer to not sell or share** their personal information, a business is **prohibited from selling or sharing** the consumer's personal information after receipt of a do not sell/share request from the consumer, unless the consumer subsequently provides consent for the sale or sharing of personal information.

Differences

GDPR	California Privacy Laws
Data subjects must be provided with information about **how to exercise** the right.	Consumers must be provided with a **'Do Not Sell or Share My Personal Information' button** on a business website (assuming it sells or shares personal information), and must be provided with several different ways to make such a request, including an address, email address, webform and/or toll-free number, depending on the company's presence.
The GDPR establishes a **right to restrict processing** where: • the accuracy of the personal data is contested by the data subject; • the processing is unlawful and the data subject opposes the erasure of the personal data; • the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject;	The CCPA and CPRA **do not** establish similar provisions. However, the CPRA gives consumers the right to direct a business to **limit its use** of a consumer's sensitive personal information to that use which is necessary to perform the services or provide the goods reasonably expected by an average consumer.

GDPR	California Privacy Laws

Differences (cont'd)

GDPR	California Privacy Laws
• pending the verification of whether the legitimate grounds of the controller override those of the data subject.	
The GDPR **does not** contain a similar provision.	A business may not sell or share the personal information of a consumer less than **16 years** of age, unless the consumer (when 13 and over) affirmatively authorises the sale or sharing of personal information. For consumers under the age of 13, express/affirmative parental consent is required to sell or share personal information.
Under the GDPR, data subjects are provided with the right to object to the processing of their personal data in specific circumstances, although this right may be limited in certain circumstances: • the processing of personal data is due to **tasks carried out in the public interest** or **based on a legitimate interest pursued by the data controller** or **third party**; • the processing of personal data is for **direct marketing purposes**; and • the processing of personal data is for **scientific, historical research or statistical purposes**.	The CCPA and CPRA **allow for businesses to ignore requests that would inhibit**: • completing transactions; • detecting security incidents; • conduct debugging; • exercising free speech; • complying with the California Electronic Communications Privacy Act; • engage in public or peer-reviewed scientific, historical, or statistical research (if the consumer has provided informed consent); • enable solely internal uses based on reasonable expectations; and • comply with legal obligations.

5.4. Right of access

The CCPA and CPRA give rights to consumers that are similar, but distinct from the GDPR's right to access. This includes disclosure rights that are granted to consumers, particularly with respect to businesses that collect personal data and businesses that sell personal data. Although similar, the laws differ slightly with respect to the procedures around responding to a consumer's request to access their data, and the CCPA/CPRA couples portability requirements when receiving a request electronically, while the GDPR carves this out as an independent right.

GDPR	California Privacy Laws
Articles 15 Recitals 59-64	Sections 1978.110 and 1798.115 of the CCPA Section 7 of the CPRA

Similarities

The GDPR recognises that data subjects have the **right to access** their personal data that is processed by a data controller.

The CCPA and CPRA both provide consumers with a **right to know** what personal information is being collected about them, as well as a **right to access** their personal information.

The GDPR specifies that, **when responding to an access request**, the data controller must indicate the following information:

- the **purposes** of the processing;
- the **categories** of personal data concerned;
- the recipients or categories of recipients to whom the personal data has been or will be **disclosed**, in particular recipients in third countries or international organisations;
- where possible, the envisaged **period** for which the personal data will be **stored**, or, if not possible, the criteria used to determine that period;
- the existence of the right to request from the controller **rectification or erasure** of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
- the right to lodge a **complaint** with a supervisory authority;
- where the personal data are not collected from the data subject, any available information as to their **source**; and
- the existence of **automated decision-making**, including profiling.

Upon receipt of a verifiable consumer request, a business that collects personal information must disclose the following to a consumer:

- the **categories of personal information** being collected;
- the **categories of sources** from which the personal information is collected;
- the **commercial purpose** for collecting, selling, or sharing personal information;
- the **categories of third parties** to whom the business discloses personal information; and
- the **specific pieces of personal information** it has collected about that consumer.

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

The CCPA and CPRA generally require at least two methods of making a request, including through a **toll-free number and online**.

GDPR	California Privacy Laws

Similarities (cont'd)

The GDPR specifies that a data controller must have in place mechanisms to for **identity verification**.

The CCPA requires that businesses are able to **verify consumer requests**.

Differences

The GDPR provides that the right of access **must not adversely affect the rights or freedoms of others**.

The CCPA/CPRA **do not** contain a similar provision.

A data controller can refuse to act on a request when it is **manifestly unfounded, excessive, or has a repetitive character**.

The CCPA/CPRA **do not** contain a similar provision.

The GDPR provides that the right of access must not adversely affect the rights or freedoms of others, **including those related to trade secrets**.

The CCPA/CPRA **do not** contain a similar provision.

The right to access 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.

Under the CCPA, business must respond to a consumers request to access their data, and must deliver the data **free of charge**. There are no express requirements as to the possible imposition of charges.

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

A business has **45 days** to respond to a consumer request for access, which can be extended an additional 45 days upon notice to the consumer.

5.5. Right not to be subject to discrimination

The GDPR does not explicitly address discrimination, although some of its provisions may be found to be based on this principle. However, the CCPA and CPRA do expressly address discrimination.

GDPR	California Privacy Laws
Articles 5, 22 Recitals 39, 71-73	Section 1798.125 of the CCPA

Similarities

GDPR	California Privacy Laws
Not applicable.	Not applicable.

Differences

GDPR	California Privacy Laws
The GDPR **does not** explicitly address the right not to be subject to discrimination; therefore, no scope of implementation is defined.	A business **shall not discriminate** against a consumer because a consumer exercised any of the consumer's rights under the CCPA or CPRA.
The GDPR **does not** contain a similar provision.	A business **may not discriminate** in any of the following ways: • denying goods or services to the consumer; • charging different prices or rates for goods/services; • providing a different level or quality of goods or services to the consumer; • suggesting that the consumer will receive a different rate, level, or quality of goods or services; or • retaliate against any employee, applicant, or independent contractor for exercising their rights.
The GDPR **does not** contain a similar provision.	A business **may offer financial incentives** for the **collection of personal information**; and may offer a different price, rate, level, or quality of goods or services to the consumer if that price or difference is reasonably related to the value provided to the business by the consumer's data.

5.6. Right to data portability

Similar to the GDPR, the CCPA and CPRA provide for the right to data portability and outline specific format requirements.

GDPR	California Privacy Laws
Articles 12, 20, 28 Recitals 68, 73	Section 1798.130 of the CCPA Section 12 of the CPRA

Similarities

GDPR	California Privacy Laws
The GDPR provides individuals with the **right to data portability**.	The CCPA and CPRA provide consumers with a **right to data portability**.
The GDPR defines the right to data portability as the **right to receive data processed on the basis of contract or consent and processed by automated means, in a 'structured, commonly used, and machine-readable format'** and to transmit that data to another controller without hindrance.	The business must provide any requested consumer data in a **readily useable format** that allows the consumer to **transmit the information from one entity to another entity without hindrance**.
Anonymous data is not subject to the GDPR, and therefore to the right to data portability.	The CCPA and CPRA **do not** specifically address **anonymous data** and there is no explicit requirement to provide this type of data to consumers.

Differences

GDPR	California Privacy Laws
The GDPR **does not** explicitly limit the scope of the right to data portability to special categories of personal data.	The CCPA/CPRA **do not** contain a similar provision.

6. Enforcement

Fairly inconsistent

6.1. Monetary penalties

Under both the GDPR and the CCPA/CPRA, monetary penalties can be issued for violations of the law. However, the penalties differ in terms of their nature, amount, and the procedure to be followed when issuing such penalties.

GDPR	California Privacy Laws
Article 83, 84 Recitals 148-149	Section 1798.155 of the CCPA Section 17 of the CPRA

Similarities

The GDPR provides for the possibility of administrative, **monetary penalties** to be issued by the supervisory authorities in cases of non-compliance.

The CCPA/CPRA provides for **monetary fines** in case of non-compliance.

When applying an administrative sanction, the supervisory authority must consider:

- the nature, gravity and duration of the infringement;
- the intentional or negligent character of the infringement;
- any action taken to mitigate the damage;
- the degree of responsibility of the controller or processor;
- any relevant previous infringements;
- the degree of cooperation with the supervisory authority;
- the categories of personal data affected by the infringement;
- the manner in which the infringement became known to the supervisory authority;
- where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;
- adherence to approved codes of conduct or approved certification mechanisms; and
- any other aggravating or mitigating factor applicable to the circumstances of the case.

With respect to consumer **relief for breaches of their nonencrypted and nonredacted personal information**, courts shall consider any one or more of the relevant circumstances presented by any of the parties to the case, including, but not limited to:

- the nature and seriousness of the misconduct;
- the number of violations;
- the persistence of the misconduct;
- the length of time over which the misconduct occurred;
- the wilfulness of the defendant's misconduct; and
- the defendant's assets, liabilities, and net worth.

Differences

Fines may be **issued directly** by supervisory authorities.

The CCPA, with some amendments from the CPRA, provides for the possibility of **administrative fines** to be issued. Additionally, the CCPA provides for a **30-day cure period** for violations, under Section 1798.155 of the CCPA, which is removed by the CPRA under Section 17 of the CPRA.

GDPR	California Privacy Laws

Differences (cont'd)

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

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.

The CCPA **does not** provide for a maximum penalty amount that can result for the imposition of several penalties for each violation. Depending on the violation, the penalty that can be issued may be up to **$2,500** for each **violation**; **$7,500** for each **intentional violation, or violations involving the personal information of consumers whom the business, service provider, contractor, or other person has actual knowledge is under 16 years of age**.

Under the GDPR, it is left to **Member States to create rules** on the application of administrative fines to public authorities and bodies.

There is not a similar provision under the CCPA/CPRA. Under the CCPA, businesses or third parties may seek the opinion of the AG for guidance on how to comply with the provisions of the law. Under the CPRA, the CPPA is responsible for **issuing regulations** which clarify compliance obligations for businesses.

6.2. Supervisory authority

Fairly consistent

An authority to supervise the application of the law and to assist organisations in their understanding and compliance efforts is provided for by both the GDPR and the CCPA/CPRA. However, the two designated supervisory authorities, the AG acting in conjunction with the CPPA as well as the EU's national data protection authorities under the CCPA/CPRA and the GDPR respectively, have different powers with respect to investigatory actions and enforcement.

Moreover, and important to note, is that the EU's national data protection authorities form part of the European Data Protection Board, which ensures the consistent application of the GDPR across Europe.

GDPR	California Privacy Laws
Articles 51-84 Recitals 117-140	Sections 1798.155, 1798.185 of the CCPA Section 24 of the CPRA

Similarities

GDPR	California Privacy Laws
Under the GDPR, supervisory authorities have **investigatory powers** which include: (i) ordering a controller and processor to provide information required; (ii) conducting data protection audits; (iii) carrying out a review of certifications issued; and (iv) obtaining access to all personal data and to any premises.	The AG and the CPPA have the power to initiate **investigations** and actions against alleged non-compliance from businesses. The CPRA provided for the creation of the **CPPA** which acts as a supervisory authority responsible for **enforcement** of the CCPA and with full **administrative power, authority, and jurisdiction**.
	The CPPA may **investigate** possible violations of the CCPA, with investigatory powers including: (i) subpoenaing witnesses, compelling attendance and testimony; (ii) administering oaths and affirmation; and (iii) taking evidence.
Under the GDPR, supervisory authorities have **corrective powers** which include: (i) issuing warnings and reprimands; (ii) imposing a temporary or definitive limitation including a ban on processing; (iii) ordering the rectification or erasure of personal; and (iv) imposing administrative fines.	Under the CPRA, the CPPA is tasked with the responsibility to **administer, implement, and enforce the law through administrative actions**. The CPPA further has **corrective powers** which include: (i) issuing cease and desists; and (ii) imposing administrative fines. It can also support this by **issuing regulations** which clarify compliance obligations.
Under the GDPR, supervisory authorities shall also handle **complaints** lodged by data subjects.	The CPPA may **investigate** possible violations of the CCPA.
Under the GDPR, supervisory authorities are tasked with **promoting public awareness** and understanding of the risks, rules, safeguards and rights in relation to processing as well as **promoting the awareness of controllers and processors** of their obligations, amongst other tasks.	Through the CPRA, the CPPA is further responsible for **protecting** the fundamental privacy rights of data subjects, **promoting public awareness** and understanding of risks, rules, safeguards, and rights in relation to the use of personal information, amongst other tasks.

GDPR	California Privacy Laws

Differences

GDPR	California Privacy Laws
It is **left to each Member State to establish a supervisory authority**, and to determine the qualifications required to be a member, and the obligations related to the work, such as duration of term as well as conditions for reappointment.	The AG and the CPPA have the power to **assess a violation** of the CCPA.
Supervisory authorities may be subject to financial control only if it does not affect its **independence**. They have separate, public annual budgets, which may be part of the overall national budget.	The monetary penalties collected through civil actions under the CCPA form the **Consumer Privacy Fund**, which funds the activities of the CPPA.
The GDPR **does not** contain a similar provision.	No administrative action brought under the CCPA will be commenced **more than five years** after the date on which the violation occurred.

6.3. Other remedies

Fairly inconsistent

Individuals are provided with a cause of action to seek damages for privacy violations under both the GDPR, and the CCPA with its amendments by the CPRA. In addition, both laws allow for class or collective actions to be brought against organisations violating the laws.

However, unlike the GDPR which allows for an action to be brought for any violation of the law, the CCPA is more restrictive and provides a cause for action only with regard to the failure of security measures and in the context of data breaches.

GDPR Articles 79, 80, 82 Recitals 131, 146, 147, 149	California Privacy Laws Section 1798.150 of the CCPA Section 16 of the CPRA
Similarities	
The GDPR provides individuals with a cause of action to **seek compensation** from a data controller and data processor for a violation of the GDPR.	The CCPA and CPRA provide individuals with a cause of action to **seek damages** for violations of the law with regard to security measures violations and data breaches.
Under the GDPR, the data subject has the right to **lodge a complaint** with the supervisory authority. The supervisory authority must inform the data subject of the progress and outcome of his or her complaint.	As detailed above, the CCPA and CPRA **provide consumers with a cause of action**, where they can institute a civil action where their nonencrypted and nonredacted personal information is subject to an unauthorised access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices.
Differences	
The GDPR allows Member States to provide for the possibility for data subjects to give a mandate for representation to a **not-for-profit body, association, or organisation** that has as its statutory objective the protection of data subject rights.	The CCPA/CPRA **do not** contain a similar provision.
The GDPR **does not** contain a similar provision.	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 violation(s). If, within 30 days and no further violation is claimed, the violation is deemed to be 'cured', and no action is initiated. 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. If a business continues to violate this law in breach of the express written statement provided to the consumer, 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 that postdates the written statement.
The GDPR **does not** contain a similar provision.	The CCPA provides for the amount of damages to be established, and outlines that **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.
The GDPR **does not** contain a similar provision.	This remedy is **only possible** when non-encrypted **and** non-redacted personal information **or where email addresses in combination with a password or security question and answer that would permit access to the account** is subject to an unauthorised access and exfiltration, theft, or disclosure as a result of the business's violation of its security obligations.
The GDPR provides that a data controller or processor shall be **exempt from liability to provide compensation** if it proves that it is not in any way responsible for the event giving rise to the damage.	The CCPA/CPRA **do not** contain a similar provision.