ROPES & GRAY

GDPR VS CCPA

	GDPR	CCPA
SCOPE		
Who needs to comply?	The GDPR applies to controllers and processors that are processing the personal data of data subjects (defined below), and are either: ▪ Established in the EU and process personal data in the context of the activities of that establishment, or ▪ Established outside the EU but offer goods or services to, or monitor the behavior of, data subjects in the EU	The CCPA applies to for-profit businesses that: ▪ Are "doing business" in California (broadly conceived) ▪ Collect or use personal information about natural persons who reside in California ▪ Determine the purposes and means of processing consumers' personal information, and ▪ Meet any of the following criteria: – Have more than $25 million in gross revenue – Buy, receive for commercial purposes, sell or share personal information of 50,000 or more consumers, households, or devices – Derive 50% or more of their annual revenue from selling consumers' personal information The law also includes provisions regarding a business's "service providers."
Exemptions	The GDPR does not apply to the processing of personal data: ▪ By a natural person (i.e., a real person, not a corporation or other entity) in the course of a purely personal or household activity ▪ In unstructured hardcopy form, or ▪ In respect to certain activities concerning national security or law enforcement	The CCPA contains several exceptions, including some relevant to certain business sectors. The CCPA shall not restrict a business's ability to: ▪ Comply with federal, state or local law, regulatory inquiries, or subpoenas exercising or defending legal claims ▪ Collect or sell consumer data if the commercial conduct takes place wholly outside of California and the individual whose data is collected is not located in California ▪ Collect, use, retain, sell or disclose de-identified or aggregate data The CCPA also includes business sector-specific exemptions for data that is subject to other regulatory regimes. These include: ▪ **Financial Services:** Data collected "pursuant to" the Gramm-Leach-Bliley Act (GLBA) and its implementing regulations

	GDPR	CCPA
SCOPE *(continued)*		
Exemptions *(continued)*		▪ **Health Care:** Protected health information (PHI) covered by HIPAA that is collected by a covered entity or business associate is exempt (as is medical information governed by California's Confidential Medical Information Act (CMIA). A provider of health care governed by the CMIA also satisfies this exemption if it treats patient information in the same manner as medical information, as defined in that act. ▪ **Clinical Trials:** Information collected as part of a clinical trial subject to the Common Rule, pursuant to good clinical practice guidelines issued by the International Council for Harmonisation or pursuant to human subject protection requirements of the United States Food and Drug Administration. ▪ **Nonprofits:** The CCPA implicitly exempts nonprofits and "noncommercial" journalism.
DEFINITIONS		
Data Subject/ Consumer	The GDPR applies to the "personal data" of a "data subject, which is any identified or identifiable natural person (i.e., real person, not a corporation or other entity) regardless of whether they are a resident of the European Union (subject to scope limitations).	▪ The CCPA applies to the "personal information" of a "consumer," which is defined more broadly than the word "consumer" would imply. A "consumer" is any natural person who is a California resident. ▪ This includes anyone in California for more than "a temporary or transitory purpose" and anyone "domiciled in the state" but "outside of the state for a temporary or transitory purpose." ▪ "Consumer" currently includes California resident employees. ▪ "Consumer" includes information about natural persons obtained in a business-to-business setting, such as people who work for California companies.
Controller/Business	A "controller" is the person or legal entity that decides the purposes and means of processing—i.e., why and how personal data is processed. Where two or more controllers together decide why and how to process the same personal data, they will be joint controllers in respect of the data.	The CCPA does not explicitly use the term "controller," but it similar to the GDPR in effect. It defines a "business" as an entity that determines the purposes and means of processing a consumer's personal information—i.e., why and how the personal information is processed.
Data Processor/ Service Provider	A "processor" is the person or legal entity that processes personal data on behalf of the controller. The processor may have some decision-making power in relation to how it processes personal data, but it will never decide why the personal data is processed.	A "service provider" is a 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."

	GDPR	CCPA
DEFINITIONS *(continued)*		
Personal Data/ Personal Information	Personal data is any information, documents or electronic data relating to an identified or identifiable natural person. ▪ An identifiable natural personal is one who can be identified, directly or indirectly, including by reference to an identifier. ▪ An identifier can include a name, identification number, customer number, location data or coordinates, an online identifier such as an IP address or cookie ID, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Sensitive personal data is a subset of personal data that must be specially protected. It is an exhaustive list that includes: ▪ Personal data that reveals an individual's race, ethnic origin, religious or philosophical beliefs, trade union membership, or political opinions, and ▪ Genetic or biometric data, data concerning a data subject's sexual lifestyle/orientation, physical or mental health, and data relating to criminal convictions and offences.	Personal information is information that identifies, relates to, describes, is capable of being associated with or could reasonably be linked, directly or indirectly, with a particular consumer or household. ▪ The CCPA does not define "household" to require a link to an individual or group of individuals, so the scope could include household data that is not linked to an individual. ▪ Deidentified or aggregate data is outside the scope of the CCPA's main provisions. Unlike the GDPR, there are no requirements specific to "sensitive" personal information.
REQUIREMENTS		
Registration/ Notification	There is no uniform EU requirement to register with or notify data protection authorities in respect of personal data processing. Some member states have introduced their own requirements—e.g., data controllers in the UK must pay an annual data protection fee to the Information Commissioner's Office.	The CCPA has no registration requirement.
Requirements for Processors/ Service Providers	Where a controller engages a processor, the parties must enter into a contract that contains provisions on (among other things) assistance, appointment of sub-processors, security and breaches, data subject rights, audits, and data transfers.	Unlike the GDPR, there are no express obligations imposed on "service providers" by the statute.

	GDPR	CCPA
REQUIREMENTS *(continued)*		
Requirements for Processors/ Service Providers *(continued)*		By contract, a business will need to enter into an agreement with the "service provider" containing certain provisions if it wishes to fit within an exception to the definition of "sale." Specifically, the contract must prohibit the service provider "from retaining, using or disclosing personal information for any purpose" other than the purpose of performing the contracted services. This means that service providers are expressly prohibited from selling or using the data they receive from businesses for a commercial purpose. Businesses may also include in their contracts an obligation for service providers to cooperate with requests that the business receives for access to or deletion of information.
Lawful Basis/ Consent	Controllers must have (and record) a lawful basis for any processing of personal data. Legal bases include necessity to perform a contract, consent, legitimate interests and compliance with law. If sensitive personal data is involved, additional conditions need to be met. Where consent is relied upon, it must be a clear affirmative indication of intent that is freely given, specific and unambiguous (i.e., not implied).	Under the U.S. Constitution's First Amendment and Article 1 of California's Declaration of Rights, there is a general presumption that businesses can process data for purposes that are not otherwise subject to restrictions, and there is not an express requirement that a business have a lawful basis for processing consumer data. Under state and federal consumer protections laws, businesses generally cannot process data in ways that are unfair or deceptive.
Data Subject Rights	Data subjects have certain rights in respect of their personal data, including the right to be informed, to access, to rectification, to erasure, to restrict processing, to data portability, to object, not to be subject to automated decision making and profiling, and to complain to a member state DPA. These rights may be subject to exceptions. For example: ▪ If fulfilling a request would reveal personal data about another person where it would infringe the rights of the controller or a third party, and ▪ If the controller is required by law to, or has a legitimate interest in, retaining personal data There is no right to object to the sale of personal data, but the controller would need to have a legal basis to do so (which likely would require consent of the data subject).	Consumers have three main categories of rights, subject to exceptions: ▪ The right to access personal information collected about them in the 12 months prior to the request – Businesses must offer at least two methods for submitting requests, including a toll-free number and an online option if the business maintains a website. – If provided electronically, it must be in a portable and easily usable format. ▪ The right to deletion of their personal information – Subject to exceptions, including for "solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business." ▪ The right to opt out of sales of their personal information

	GDPR	CCPA
REQUIREMENTS *(continued)*		
Rights: Process	Controllers must comply with requests within one month of receipt, but can extend this period by a further two months where: ▪ The processing is carried out by a public authority or body ▪ Their core activities involve regular and systematic monitoring of data subjects on a large scale, or ▪ Their core activities involve processing of sensitive personal data/ criminal convictions or offences data on a large scale	Businesses must respond to consumers' requests within 45 days from the receipt of the request, but that deadline can be extended 45 days when reasonably necessary if the business gives the consumer notice of the extension within the first 45 days. Another provision suggests that the period may be extended by up to 90 days. This inconsistency may be resolved in future drafts.
Sale of Personal Data	There are no general restrictions on the sale of personal data under the GDPR. However, data controllers must comply with the principles of the GDPR, including fairness and having a lawful basis for the processing.	Business that "sell" personal data must give consumers the right to opt out of that sale and must include a clearly labeled "Do Not Sell My Personal Information" link on their homepage. The definition of "sell" or "sale" is broader than what many consider typical sales, i.e., an exchange for money. Under the CCPA, a sale includes any transfer or communication of personal information "by the business to another business or a third party for monetary or other valuable consideration." Transfers to service providers are not considered sales, provided appropriate contractual restrictions are in place.
Children	A parent or guardian's consent is required to process personal data for children under 16, but member states may lower the age to 13.	For children under 13, a parent or guardian must opt in to the sale of their personal information. Minors who are 13 to 16 years old may opt in to the sale of their own personal information.
Nondiscrimination	Nondiscrimination is not specifically covered in the GDPR the way it is under the CCPA. However, many of the GDPR's principles of processing reach the same kind of conduct. For example, under the GDPR, consent must be freely given and is revocable, so businesses cannot deny goods or services to data subjects if they refuse to provide consent to processing or withdraw that consent.	Businesses are expressly prohibited from discriminating against consumers who exercise their rights under the CCPA, including in any of the following ways: ▪ Denying those consumers goods or services ▪ Charging those consumers different prices or rates ▪ Providing a different quality of goods or services, and ▪ Offering a discount for goods or services if the consumers choose not to exercise their rights A business can offer financial incentives to the consumer for the collection or sale of their personal information and can charge them a different price or level of service if the difference is directly related to the value of the data.

	GDPR	CCPA
REQUIREMENTS *(continued)*		
Documentation/ Accountability	Controllers and processors must implement a range of measures to comply with—and demonstrate that they comply with—the GDPR, which may require extensive documentation, including: ▪ Internal policies and procedures ▪ Detailed records of processing ▪ Data protection impact assessments ▪ Data protection by design and default, and ▪ Staff training	The CCPA does not have the same documentation requirements as the GDPR. Businesses are required to verify that anyone responsible for handling consumer requests are informed about the CCPA requirements and can provide consumers instructions for exercising their CCPA rights, which will likely require some training. Documentation is often otherwise appropriate as a compliance best practice. For example, although a record of processing is not expressly required by the CCPA, creating a data map or inventory can be an important step toward fully understanding what data a business collects and how it is used, which is essential for CCPA compliance.
Data Protection Officers	Controllers and processors must appoint a data protection officer where: ▪ The processing is carried out by a public authority or body ▪ Their core activities involve regular and systematic monitoring of data subjects on a large scale, or ▪ Their core activities involve processing of sensitive personal data/ criminal convictions or offences data on a large scale Member states may introduce their own requirements—e.g., in Germany, controllers and processors who employ 10 or more individuals involved in data processing must appoint a DPO.	No officials or officers need to be desginated.
Security Breach Notification	Controllers must report personal data breaches to data protection authorities within 72 hours where the breach poses a risk to data subjects' rights and freedoms, and to data subjects without undue delay where the breach poses a high risk to their rights and freedoms. Processors must report personal data breaches to controllers without undue delay (all breaches that meet the GDPR's threshold must be reported).	California's pre-existing state data breach notification law continues to apply, which requires businesses to report personal information breaches to consumers "without unreasonable delay." California state regulators must be notified if more than 500 California residents are notified. The CCPA also creates a private right of action with statutory damages of between $100-$750 per consumer per incident arising from certain data breaches where a business has not implemented reasonable security procedures and practices appropriate to the nature of the information to protect the personal information.

	GDPR	CCPA
REQUIREMENTS *(continued)*		
Data Security	Controllers and processers are required to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk to personal data, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing.	Although there is no express data security requirement, the CCPA creates a private right of action arising from data breaches where the business has failed to implement "reasonable security procedures and practices appropriate to the nature of the information to protect the personal information."
International Transfers	Transfers of personal data outside the European Economic Area are restricted other than: ▪ To countries deemed by the European Commission to offer "adequate" protection for personal data (the United States is not included in this list) ▪ Where Commission-approved model clauses or another transfer mechanism (e.g., binding corporate rules or the EU-U.S. Privacy Shield) are in place, or ▪ Where there is an exception in the GDPR (e.g., explicit consent, contractual necessity, or to establish or defend legal claims)	The CCPA does not restrict international data transfers.
ENFORCEMENT/LITIGATION		
Regulatory Enforcement	Data protection authorities may issue a range of penalties, including: ▪ Fines of up to the greater of €20 million or 4% of annual worldwide turnover (and will extend to undertakings and, potentially, parent companies) ▪ Requiring organizations to amend their processing practices, and ▪ Requiring organizations to stop processing data altogether	Businesses that violate the CCPA may be liable for a civil penalty of up to $2500 for each violation or up to $7500 for each intentional violation. Businesses are given 30 days to cure any alleged violations.
Private Rights of Action	Data subjects have a range of rights against controllers and processors, including lodging complaints with data protection authorities, bringing direct claims for compensation and instructing representative bodies to bring class action claims on their behalf.	The CCPA creates a private right of action related to certain data breaches where a business fails to implement reasonable security procedures. The private right of action provides for statutory damages of between $100–$750 per consumer (or actual damages, whichever is greater). There is not a separate right of action to enforce the other terms of the CCPA.