BakerHostetler

California Consumer Privacy Act (CCPA) as amended by SB 1121

vs. European Union General Data Protection Regulation (GDPR)

	CCPA	GDPR	Comparison
Effective	Jan. 1, 2020, but to be able to comply with the effective date, Businesses (defined below) will need to start tracking data practices on Jan. 1, 2019. The August amendments of SB 1121 delay attorney general enforcement until the later of six months from regulations or July 1, 2020.	May 25, 2018	GDPR is currently in effect, but only limited guidance as to its proper interpretation has been published to date (e.g., e-Privacy Regulation has not yet been finalized). The CCPA has yet to come into effect and may be further amended before its effective date.
Who Is Regulated	Any "**Business**" that is a for-profit entity, doing business in California, that: • Has a gross revenue in excess of $25 million; or • Annually buys, receives for the business's commercial purposes, sells or shares for commercial purposes the Personal Information (PI) of 50,000 or more Consumers (defined below), households or devices [e.g., this amounts to 137 credit card transactions a day or 137 unique website visitors a day]; or • Derives 50 percent or more of its annual revenues from selling Consumers' PI. **OR**, an entity that: • Controls or is controlled by a Business that does any of the above and shares common branding with that business. "Controls" means ownership of, or the	**Any organization** that: • Is "established" in the EU; • Offers goods or services in the EU; or • Monitors or tracks the behavior of EU data subjects within the EU.	Substantially different.

 The California legislature is considering amendments to the CCPA. ***SB 1121 amending the Act passed on August 31, and was signed into law on September 23***. *Further* amendments are expected. This chart is current as of September 26, 2018. For more information contact AFriel@BakerLaw.com or LJehl@BakerLaw.com. This chart is a top level summary for issue spotting purposes and is not legal counsel. See www.dataprivacymonitor.com for CCPA updates.

	CCPA	GDPR	Comparison
	power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business; control in any manner over the election of a majority of the directors, or of individuals exercising similar functions; or the power to exercise a controlling influence over the management of a company. "Common branding" means a shared name, service mark or trademark. **BUT**: Does not apply to commercial conduct taking place wholly outside of California – for example, where a Business collects PI while the Consumer is outside of California, no part of the sale of the Consumer's PI occurred in California, and no PI collected while a Consumer was in California is sold. The CCPA does not, however, permit a Business to store, including on a device, PI about a Consumer when the Consumer is in California and then to collect that PI when the Consumer or stored PI is outside of California. This exception will have limited applicability, and most national Businesses, including e-commerce sites headquartered out of state, should expect to be covered.		
	In addition to regulating Businesses, parts of the CCPA apply specifically to: "**Service Provider**": A sole proprietorship, partnership, limited liability company, corporation, association or other legal entity that is organized or operated for the profit or	An organization that does any of the above is categorized as either: "**Controller**": Any natural or legal person, public authority, agency or other body that, alone or jointly with others, determines the	Substantially different, both in parties regulated and in how they are regulated. The GDPR requires entities that handle PI/personal data on behalf of another to be governed by contracts that contain specific data

	CCPA	GDPR	Comparison
	financial benefit of its shareholders or other owners, that processes information ***on behalf*** of a Business and to which the Business discloses a Consumer's PI **for a business purpose** [but NOT for a commercial purpose] ***pursuant to a written contract***, provided that the contract prohibits the entity receiving the information from retaining, using or disclosing the PI for any purpose other than for the specific purpose of performing the services specified in the contract for the Business, or as otherwise permitted by this title, including retaining, using or disclosing the PI for a commercial purpose other than providing the services specified in the contract with the Business. **And:** "**Third Party**": Any person who is not a Business or a Service Provider, as long as the Service Provider's written contract includes a ***certification*** made by the Service Provider that it understands the restrictions required in the written contract [described above] and will comply with them. Service Providers that include a ***certification*** in the written contract and that violate any of the restrictions shall be liable. A Business that discloses PI to a violating Service Provider is not liable, provided that, at the time of disclosing the PI, the Business does not have actual knowledge, or reason to believe, that the Service Provider intends to commit such a violation. A Business can be both a Business and a Service Provider, but it cannot be both a Business and a Third Party. A	purposes and means of the processing of personal data. **Or**: "**Processor**": any natural or legal person, public authority, agency, or other body that processes personal data ***on behalf*** of a Controller. An organization can be both a Controller and a Processor, depending on the purposes for processing personal data. The GDPR ***requires a contract*** or other legal act under EU Member State law to govern Processors' processing on behalf of Controllers. The contract must set out the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, and the obligations and rights of the Controller. The contract must also stipulate that the Processor: • May process the personal data only on documented instructions from the Controller, including with regard to transfers of personal data to a third country or an international organization, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the	protection provisions, whereas the CCPA requires this only of Business's engagements of business-purposes vendors that meet the definition of a Service Provider, and not other types of vendors or other Third Parties.

	CCPA	GDPR	Comparison
	Service Provider can be both a Service Provider and a Third Party as long as it ***does not include a certification*** in the written contract. Business purposes are limited by definition to certain internal operational purposes, whereas commercial purposes are purposes that "advance a person's commercial or economic interests." A vendor that collects/receives/processes PI for its own or the Business's commercial purposes is a Third Party and not a Service Provider. The CCPA governs Third Parties by limiting their ability to resell PI obtained through a sale from a Business without giving explicit notice and providing the opportunity to opt out to Consumers, but otherwise does not regulate them unless they are also a Business. Businesses must make certain disclosures regarding Third Parties that do not apply to Service Providers. Businesses must require Service Providers to delete PI upon a Consumer's request to the Business, but do not have the same requirement with regard to Third Parties. **Change of Control** If a Business is sold or sells its assets, the successor party may receive the associated PI, but must give Consumers notice of any changes to the data practices from what was provided in CCPA-required notices and disclosures.	Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest; • Will ensure that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality; • Will take all required security measures; • Respects the requirements that the Processor (1) will need prior written authorization from the Controller in order to engage another Processor, (2) will give the Controller the opportunity to object to any additional Processors, (3) will impose the same data protection obligation contained in its contract with the Controller onto the additional Processor via a contract that provides guarantees of implementing appropriate technical and organizational safeguards for the data deemed sufficient under the GDPR, and (4) will be fully liable to the Controller if the additional Processor fails to meet obligations; • Will assist the Controller in responding to data subject rights requests;	

	CCPA	GDPR	Comparison
		• Will assist the Controller in ensuring compliance with GDPR requirements on security, data breaches, Data Protection Impact Assessments and consulting supervisory authorities; • As directed by the Controller, deletes or returns all the personal data to the Controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data; and • Will make available to the Controller all information necessary to demonstrate compliance and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller.	
Who Is Protected	"**Consumers**," who are defined as California residents, includes (1) every individual who is in the State for other than a temporary or transitory purpose, and (2) every individual who is domiciled in the State who is outside the State for a temporary or transitory purpose, however identified, including by any unique identifier. This definition is partially defined in Section 17014 of Title 18 of the California Code of Regulations (residency for state tax purposes), as that section read on Sept. 1, 2017. Consumers include but are not limited to customers of household goods and services, a departure from other	"**Data subjects**," who are natural persons who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data or 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.	Substantially different in approach, but similarly broad in effect.

	CCPA	GDPR	Comparison
	California privacy laws. Thus, employees are covered, as are B-to-B transactions.		
What Is Data?	"**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. PI may include, but is not limited to, the following categories (which categories must be used when providing required notices and disclosures): • 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. • Signature, physical characteristics or description, address, telephone number, state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information or health insurance information. • Characteristics of protected classifications under California or federal law (e.g., race, gender, sexual orientation, etc.). • Commercial information, including records of personal property, products or services purchased, obtained or considered, or other purchasing or consuming histories or tendencies.	"**Personal Data**" is broadly defined as any information that permits identification of a data subject, directly or indirectly. Examples: name, identification number, location data, online identifier such as IP address, or reference to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the data subject. "**Special categories of personal data**" are 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. **Does include** "pseudonymous data" as "personal data." **Does not include** "aggregate" data or "anonymous information" as "personal data." **Does not mention** deidentified data.	Substantially similar. Both definitions define the data in broad terms as information that can identify an individual directly or indirectly, though the CCPA's is arguably broader in general language and by examples given. Each definition provides examples, some of which overlap. There are nuances to each definition, such as the CCPA's exclusion of "publicly available" information (from the government used for a compatible purpose) and CCPA's longer, and more specific, list of possible examples. **Please note** that both laws are in their infancy (the GDPR became effective May 25, 2018; the CCPA will become effective Jan. 1, 2020), and regulatory guidance as to specifics of what defines PI/personal data has not yet been issued.

	CCPA	GDPR	Comparison
	• 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 (20 U.S.C. Section 1232g, 34 C.F.R. Part 99). • Inferences drawn from any of the information identified in this subdivision to create a profile about a Consumer reflecting the Consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities and aptitudes. **Excludes** "publicly available" information from public government records, but explicitly does not include biometric data collected without the Consumer's knowledge and data used for an incompatible purpose as		

	CCPA	GDPR	Comparison
	publicly available. **Carve-outs** for protected health information governed by California and federal health information privacy laws and in some circumstances data regulated by certain other California or federal privacy laws (e.g., Gramm-Leach-Bliley for financial institutions). **Unclear** whether pseudonymous data, deidentified data and aggregate data are considered PI, but such data is excluded from the restrictions on collection, use, retention, sale and disclosure. Notice and information request response requirements potentially still apply.		
Privacy Notice Requirements	**-Similarities-**		
	A Business must track PI collected, and inform Consumers at or before collection, of the categories of PI collected and the purposes (business purposes and commercial purposes) for the collection of each category, and limit the use to those purposes absent further advance notice. A Business must provide the following information to Consumers in a form readily accessible to them: • A description of Consumers' rights under the CCPA, which shall be in the Business's online privacy policy (if any) and in any California-specific privacy notices; • A link to the Business's "Do Not Sell My Personal Information" web-based opt-out tool on both the Business's internet home page and in its online privacy policy (if any) and in any California-specific privacy notices;	Controllers must disclose, at the time of collection: • What personal data is to be collected and for what purposes and a description of data subject request rights; • Identity and contact details of Controller, Controller's representative and Data Protection Officers unless an exception under Art. 13 applies; • Purposes of processing; • Legal basis for processing;	Both the CCPA and the GDPR require disclosure at the time of collection. Similar requirements as to Consumer/ data subject rights disclosures, though those rights differ. CCPA requires certain disclosures to be online. Both require disclosures regarding off-line data collection.

	CCPA	GDPR	Comparison
	• Two or more designated methods for submitting information requests, including at minimum a toll-free number and a website address if the business has a website, excepting that in any online privacy notices only one additional method (i.e., toll-free number) beyond the website method need be listed. Further, a Business must provide information about the following to Consumers in any online privacy policies and any specific privacy notices to California residents, or otherwise on the Business's website: • Consumers' rights under the CCPA; • A list of categories of PI collected in the preceding 12 months and the purposes (business purposes and commercial purposes) therefor – use of another purpose requires further notice prior to different use; • If it sells PI, how that PI may be sold and how to opt out of the sale of PI; • A list of the categories of PI sold in the preceding 12 months (or if the business has not sold Consumers' PI in the preceding 12 months, the business must inform the Consumer of that fact); • A list of the categories of PI disclosed for a business purpose in the preceding 12 months (or if the business has not disclosed Consumers' PI for a business purpose in the preceding 12 months, the business must state that). The CCPA is inconsistent as to whether there is any obligation to include a list of categories of PI disclosed for a commercial purpose in the preceding 12 months in the privacy policy, but such is required to be explained in	• Legitimate interests of Controller or third party; • Third parties with whom the data will be shared, or categories of those recipients; • Any cross-border transfers and legal mechanisms; • Data retention period or criteria used to determine that period; • Data subject rights and right to withdraw; • Right to lodge a complaint with supervisory authorities; • Whether provision of personal data is a statutory or contractual obligation and possible consequences of failure to provide such data; • Existence of automated decision-making, including profiling; and • Whether personal data about a data subject was not obtained directly from the data subject, from which source the personal data originated, and whether it came from publicly accessible sources, unless an exception under Art. 14 applies.	

	CCPA	GDPR	Comparison
	response to a specific Consumer request. Accordingly, inclusion in the privacy policy is recommended; • The CCPA is also internally inconsistent as to whether the online notice needs to include the categories of sources from which PI is collected, the categories of Third Parties with which PI is shared, and the specific pieces of PI collected about a specific Consumer. Obviously, the last could not be done in a general notice. However, it is recommended that the other information be included in the online notice; and • Any financial incentives for providing data or not exercising rights. **Third Parties**, even if not a Business, need to give Consumers explicit notice and an opportunity to opt out prior to reselling their PI that was sold to the Third Party by a Business.		
	-Differences-		
	If a Business has a website, some disclosures and choice mechanisms must be made available via a website. Limits disclosures to a 12-month look-back. Treats processors differently – Service Providers (business purposes) vs. Third Parties (commercial purposes).	Disclosure need not be online. Can be written, online, or given in another way as long as transparent, intelligible and easily accessible. Disclosure must be given verbally if requested by verified data subject. Disclosure must be child-friendly if personal data is being collected from children under the age of 16. No look-back limits. Disclosure requirements more detailed (see above).	CCPA requires some disclosures to be online, while the GDPR does not require any disclosure to be online. CCPA limits disclosures to only having to provide information for the past 12 months, while the GDPR has no look-back limitations. The GDPR requires disclosure of significantly more detailed information, including the identity of

	CCPA	GDPR	Comparison
			any third parties with whom the data will be shared. Note that while the GDPR does not explicitly require disclosure of exact cookies and tracking technologies, such disclosure may be required in order to obtain a proper legal basis for processing, such as consent. Other types of information may be affected similarly under the GDPR.
Security	Any Consumer whose nonencrypted or nonredacted PI of a certain type (more narrowly defined than PI otherwise under the CCPA) is subject to an unauthorized 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 appropriate to the nature of the information to protect the PI may institute a civil action after notice and opportunity to cure [see Remedies/Penalties section below].	Appropriate technical and organizational measures to ensure a level of security appropriate to the risk.	Both CCPA and GDPR expect reasonable security measures. CCPA provides a private right of action in the event of a specific type of data breach, and existing California law provides the underlying security and incident response obligations, which laws can also support a different private cause of action.
Children	Prohibits selling PI of a Consumer under 16 years of age, unless affirmatively authorized by the minor aged 13-16, or by a parent for children under 13. A Business that willfully disregards the Consumer's age shall be deemed to have had actual knowledge of the Consumer's age.	Treatment of personal data from those aged 13-16 may vary depending on the EU Member State. Children must be given a privacy notice that they would understand based on their age and capacity to understand.	Substantially different, other than ages involved.

	CCPA	GDPR	Comparison
		Children's personal data is subject to heightened security requirements. Children are entitled to the same data subject rights as adults, though parents may make rights requests on behalf of the child if the child is under the age of consent in the applicable EU Member State.	
Request Rights	**-Similarities-**		
	Right to request disclosure, including specifics of a particular Consumer's PI, and to obtain portable copies of it. Right to delete PI, which may be limited to only the information the Business has collected, subject to limited exceptions. Businesses require that their Service Providers also delete PI upon a Consumer request to the Business; but due to the definition of Service Provider, this does not apply to vendors engaged for commercial purposes. Upon a verified request from the Consumer, a Business must provide the following information to the Consumer on an individualized basis (i.e., specific to his or her data): • The categories of PI collected about that specific Consumer; • The categories of sources from which the PI is collected; • The specific pieces of PI collected about that Consumer;	Right to request disclosure, including specifics of a particular data subject's personal data. Right to erasure of personal data, which extends to any personal data processed, including by third parties. Right to access personal data, including to view the personal data being processed. Right to data portability: Where the processing is done by automatic means and the legal basis is either consent or a contract, the data subject may request to either (1) receive the personal data concerning him or her, which he or she has provided to a Controller, in a structured, commonly used and machine-readable format and have the right to transmit that data to another Controller without hindrance from the	Similar rights to disclosure and data deletion. GDPR's right to erasure is likely more broad than CCPA's right to deletion. Both CCPA and GDPR allow information on data collected to be provided in a readily usable format, but the GDPR provides a specific right to data portability that allows data subjects to directly transfer their personal data between data Controllers. Note that the CCPA and the GDPR both allow access to information, but the CCPA's right is solely to obtain a written disclosure of the information, while the GDPR allows broader access,

	CCPA	GDPR	Comparison
	• The business purpose(s) and commercial purpose(s) for collecting or selling the PI; • The categories of Third Parties (which includes differently branded affiliates, and possibly similarly branded affiliates, but does not include Service Providers engaged for business purposes if certain requirements are met, but does include vendors for commercial purposes) with which the business "shares" PI; • For PI that is disclosed for a business purpose, the categories of the Consumer's PI that were disclosed. There is no obligation to include in an information request response information on PI disclosed for commercial purposes that are not a sale, though that may be added before the effective date and it is suggested that this also be provided; and • For PI that is sold, the categories of the Consumer's PI sold to what categories of Third Parties, and the categories of the Consumer's PI sold to each applicable Third Party (likely including affiliates). Note the distinction between Third Party sharing and business purposes disclosures. The result is that for Service Providers, a Business needs to provide categories of PI provided, but not categories of Service Provider; whereas for commercial purposes vendors, the Business must provide categories of third-party recipients, but not the categories of PI shared. When PI is sold, the customer is entitled to both categories of recipient and what categories of PI went to each such recipient category.	Controller to which the personal data have been provided, or (2) have the data Controller transfer the personal data directly to another data Controller. Data subjects may authorize another person or entity to exercise rights on their behalf, such as in the case of children under the age of consent in their respective EU Member State and when authorizing a nonprofit or public-interest third party to exercise the data subject's right to lodge a complaint and to remedies.	which is not limited to a written disclosure in a portable format. Both CCPA and GDPR allow authorized third parties to exercise rights of consumers/data subjects on their behalf, but the GDPR has additional nuances.

	CCPA	GDPR	Comparison
	A Consumer may opt out of the sale of their personal PI, and may authorize another person to opt out of the sale of the Consumer's PI on the Consumer's behalf, and a Business shall comply with an opt-out request, pursuant to regulations to be adopted by the attorney general.		
	-Differences-		
	When a Consumer opts out of the sale of PI, a Business must not request that the Consumer authorize sale for at least 12 months.	Right to rectification of personal data. Right to restrict processing of personal data, under certain circumstances. Right to object to processing for profiling, direct marketing and automated individual decision-making purposes. Right to lodge a complaint with a supervisory authority.	CCPA specifically gives the right to object to the sale of data, while the GDPR does not, although the GDPR provides far more rights, some of which have a similar effect. Further, the GDPR requirement of consent to collect, use and share personal data for nonessential purposes, such as third-party marketing, makes the need for an opt-out of most transactions that would be a sale under the CCPA effectively unnecessary.
Responding to Rights Requests	A Business must verify the Consumer making a request (portability, deletion or information), pursuant to regulations yet to be adopted by the California attorney general.	Data Controller must verify data subject's identity and rights according to the GDPR's expectations. For example, data Controllers should use all reasonable measures to verify the identity of a data subject who requests access, in particular in the context of online services and online identifiers. A Controller	Both CCPA and GDPR require verification of requests. CCPA requires the requests to be free, and the GDPR potentially allows fees to apply, depending on circumstances.

	CCPA	GDPR	Comparison
	Most requests are limited to twice a year and to a 12-month look-back, but no limits on deletion and do-not-sell requests. Must ordinarily be free to Consumer and cannot require account registration. Disclose and deliver the required information to a Consumer free of charge within 45 days of receiving a verifiable request from the Consumer. The Business shall promptly take steps to determine whether the request is a verifiable request, but this shall not extend the Business's duty to disclose and deliver the information within 45 days of receipt of the Consumer's request. The time period to provide the required information may be extended once by an additional 45 days when reasonably necessary, provided the Consumer is provided notice of the extension within the first 45-day period. A Business need not retain PI collected for a single, one-time transaction if not sold or otherwise retained, to comply with requests, and need not re-identify data to comply with requests.	should not retain personal data for the sole purpose of being able to respond to potential requests. Additionally, the GDPR requires verifying parental identity, taking into consideration available technology, if a parent is requesting on behalf of a child. Data does not have to be free to data subjects, if compliance with request is unduly onerous. The Controller should respond to requests from the data subject without undue delay and at the latest within one month, and must give reasons where the Controller does not intend to comply with any such requests. Processors, taking into account the nature of the processing, assist the Controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of the Controller's obligation to respond to requests for exercising the data subject's rights.	CCPA has strict timeline rules, and GDPR has a loose response time expectation. GDPR obligations depend on status as a Controller or Processor, whereas CCPA obligations apply to Businesses and, to a more limited extent, Service Providers and Third Parties that are sold PI by a Business and wish to resell it.
Data Rights Exceptions	A Business or a Service Provider shall not be required to comply with a Consumer's request to delete the Consumer's PI if it is necessary for the Business or Service Provider to maintain the Consumer's PI in order to: • Complete the transaction for which the PI was collected, provide a good or service requested by the Consumer, or reasonably anticipated to be needed within the context of a Business's ongoing	An organization does not need to comply with a data subject's request to exercise a right if the lawful basis for processing is: • Necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;	CCPA has exceptions to complying with the CCPA that are only limited to the right to deletion, as well as exceptions that apply to the application of various or all of CCPA's obligations on a Business. GDPR's exceptions apply to any exercise of data subject rights, but in

	CCPA	GDPR	Comparison
	business relationship with the Consumer, or otherwise perform a contract between the Business and the Consumer; • Detect security incidents; protect against malicious, deceptive, fraudulent or illegal activity; or prosecute those responsible for that activity; • Debug to identify and repair errors that impair existing intended functionality; • Exercise free speech, ensure the right of another Consumer to exercise his or her right of free speech, or exercise another right provided for by law; • Comply with the California Electronic Communications Privacy Act pursuant to Chapter 3.6 (commencing with Section 1546) of Title 12 of Part 2 of the Penal Code (warrants and government requests for information); • Engage in public or peer-reviewed scientific, historical or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the Business's deletion of the information is likely to render impossible or seriously impair the achievement of such research, if the Consumer has provided informed consent; • Enable solely internal uses that are reasonably aligned with the expectations of the Consumer based on the Consumer's relationship with the Business; • Comply with a legal obligation; and/or • Otherwise use the Consumer's PI, internally, in a lawful manner that is compatible with the context in which the Consumer provided the information.	• Necessary for compliance with a legal obligation to which the Controller is subject; • Necessary in order to protect the vital interests of the data subject or of another natural person; • Necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller; and/or • Necessary for the purposes of the legitimate interests pursued by the Controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject that require protection of personal data, in particular where the data subject is a child.	practice these exceptions may be more difficult to apply, especially if the original lawful basis for processing was consent.

	CCPA	GDPR	Comparison
	In addition, CCPA obligations on a Business shall not restrict a Business's ability to: • Comply with law or legal process; • Engage in good faith cooperation with law enforcement; and/or • Collect, use, retain, sell or disclose Consumer information that is deidentified or converted to aggregate Consumer information. Further, CCPA shall not apply to the extent it conflicts with various specified existing federal privacy and regulatory laws, or evidentiary privilege. CCPA does not apply to PI collected, processed, sold or disclosed under GLBA or the California Financial Information Privacy Act or protected health information collected by a covered entity or business associate governed by HIPAA or medical information governed by the California Confidentiality of Medical Information Act (CMIA). CCPA does not apply to a CMIA provider or a HIPAA-covered entity to the extent it maintains patient information in the same manner as medical information, or protected health information, is to be treated under CMIA and HIPAA.		
Remedies/ Penalties	Any Consumer whose nonencrypted or nonredacted PI that is part of a designated subset of PI (e.g., name and Social Security number) is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the Business's violation of the duty to implement and	Data subjects have the right to lodge a complaint with a supervisory authority; right to an effective judicial remedy against a supervisory authority, Controller or processor;	Substantially different in approach, but violations of either could potentially result in significant economic liability.

	CCPA	GDPR	Comparison
	maintain reasonable security procedures and practices appropriate to the nature of the information to protect the PI may institute a civil action for any of the following: • To recover damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty dollars ($750) per Consumer per incident or actual damages, whichever is greater. • Injunctive or declaratory relief. Actions pursuant to this section may be brought by a Consumer only if the Consumer gives the Business 30 days' notice of the CCPA violation(s) (though security is not even an express obligation under the CCPA) and gives the Business the opportunity to cure the violation(s) during such 30-day period (though it's unclear how a data breach can be cured). The August amendment of SB 1121 did away with an original obligation that the Consumer bringing an action notify the attorney general within 30 days that the action has been filed and the attorney general's right to intervene. The CCPA does not allow for a private right of action for violations of the privacy provisions of the CCPA, and provides that "[n]othing in this title (Title 1.81.5) shall be interpreted to serve as the basis for a private right of action under any other law[,]" which seems to prohibit use of the unfair business practices law (B&P Sec. 17200) to support a private claim based on violation of the CCPA. However, under existing California data protection law (Title 1.81), a more limited group of "customers" may also bring a civil action (i) limited to actual damages for data security failures; and (ii) for actual damages and statutory	and right to compensation and liability, such as when an organization's actions result in a material or nonmaterial damage due to an infringement. Administrative fines can reach 20 million euros or 4 percent of annual global revenue, whichever is highest. EU Member States can impose their own penalties.	

	CCPA	GDPR	Comparison
	damages for violation of notice and choice rights regarding sharing of PI with Third Parties for their own direct marketing purposes (the Shine the Light Act), both without need to give an opportunity to cure. The California attorney general may also bring actions for injunctive relief and for civil penalties of $2,500 per violation, or up to $7,500 per violation if intentional, after notice and a 30-day opportunity to cure. The SB 1121 amendments provide that attorney general enforcement will be delayed until the earlier of six months from issuance of regulations or July 1, 2020. The California Department of Justice has stated that it will need approximately 57 full-time staff to enforce the law and that it will need to secure over $57.5 million annually in civil penalties to cover the cost thereof.		
Consumer/ Data Subject Retaliation	A Business shall not discriminate against a Consumer because the Consumer exercised any rights. For example, a Business cannot: • Deny goods or services to the Consumer; • Charge different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties; • Provide a different level or quality of goods or services to the Consumer, if the Consumer exercises the Consumer's rights under this title; or • Suggest that the Consumer will receive a different price or rate for goods or services or a different level or quality of goods or services.	The GDPR does not explicitly state that organizations cannot discriminate against a data subject who exercises his or her rights, but such a prohibition is strongly implied throughout the text, including references prohibiting processing that adversely affects the rights and freedoms of data subjects.	Similar idea, different obligations.

	CCPA	GDPR	Comparison
	Except, however, a Business may charge differently "if that difference is reasonably related to the value provided to the consumer [sic? – Business] by the Consumer's data." A Business may also offer financial incentives based on the same value proposition. Financial incentives must be disclosed in an online privacy policy or terms, and require opt-in consent.		
Other	Requires opt-in consent for selling PI of minors under age 16 and for financial incentive programs. Businesses may seek guidance from the California attorney general for compliance advice. As a result of the SB 1121 amendments, the attorney general will have until July 1, 2020, to promulgate regulations "to further the purposes of this title," and specifically regarding how opt-outs should be facilitated and governed and how notices and information request responses should be made and requestors should be verified. Pre-empts local laws.	Requires lawful basis for processing personal data; consent is one of the lawful bases. Organizations may seek guidance from EU Member State supervisory authorities and the European Data Protection Board for compliance advice. GDPR is always subject to EU Member State laws.	GDPR is significantly more expansive than the CCPA and includes detailed provisions on issues that may or may not minimally overlap with the CCPA. For example, the GDPR considers cross-border data transfers, something the CCPA does not, but the GDPR also considers special treatment of personal data used for research and public interest purposes, similar to the CCPA provision that allows Businesses to not delete information for research purposes. GDPR requires consent to collect device or other unique identifiers, and related usage data, for profiling and interest-based advertising. CCPA's rights to opt out of sales of such data and to delete such data likely result in a mandatory opt-out of some but not all interest-based advertising data collection, retention and sharing.