PRIVACY COMPANY

CCPA versus GDPR

High level comparison

Reach & Governance		
	GDPR	**CCPA**
Reach	Broad - GDPR covers all of the European Union Member States. Applies to organisations located within the EU and organisations outside the EU that offer goods or services to EU data subjects	Narrow - Covers California residents. Obligations for organisations in California with >25 million dollar turnover, or processing data from >50k individuals, households or devices or >50% of the turnover is generated from personal data that is collected, transferred or sold
Data subjects	Protect data privacy rights of EU citizens	Protect consumers from the collection, transfer and sales of personal data for residents of the state California, consumer and household
Roles	Controller, processor, sub-processor, DPO	Service Provider (~processor), 3rd party
Supervising authority	National DPA	Attorney General
Penalties	Up to €10 million, or 2% of the firm's worldwide annual revenue from the preceding financial year / up to €20 million, or 4% of the firm's worldwide annual revenue from the preceding financial year	Maximum penalty of $2500 up to $7500 fined by the AG per incident, private parties can get between $100 and $750

Personal Data		
	GDPR	**CCPA**
Internal vs external	Between parties and internal personal data exchange	Between parties, not internal data exchange
Personal data	Personal data, including special personal data and public information	All personal data, no special categories Excluded, covered in other legislation: - medical personal data = HIPAA - public information
Children	Age <16 agreement by parents or guardians, member states can lower to 13	Age <13 consent given by parents or guardian, 13-16 can give consent themselves
Pseudonymization	Personal data after pseudonymization is still personal data	Personal after pseudonymization is NO personal data

PRIVACY COMPANY

CCPA versus GDPR

High level comparison

Data Subject Rights and accountability		
	GDPR	**CCPA**
Right to notice	Privacy Statement on website	Privacy Notice on website, opt-out from sales of personal data on website
Data Subject Rights	Right to be informed, right of access, right to rectification, right to erasure/to be forgotten, right to restrict processing, right to data portability, right to object and rights in relation to automated decision making and profiling Personal data can only be processed with legal ground, no opt-out for personal data In theory, unlimited data subject requests	Right to be informed, right of access and deletion. No right to rectification, no right to erasure/to be forgotten, no right to restrict processing, no right to data portability, no right to object and rights in relation to automated decision making and profiling Opt-out on selling your personal data (allowed unless), opt-out for marketing purposes. Max 2 data subject requests per organisation per year No B.I. profiling data (scope is limited to data that is bought/received/transferred/sold)
Due date DSR	1 month to hand over the personal data, option for 1 month extension	45 days response time, 45 – 90 days to hand over the personal data
Accountability	Obligations for record of data processing, register of data breaches	No strict obligations for accountability, until complaints are filed
DPIA	DPIA's mandatory	No DPIA's
Data breaches	Data breaches: record and follow up governed by the GDPR	Data breaches are not governed by the CCPA, but under the civil code S1789

The California Consumer Privacy Act (CCPA) is a bill meant to enhance privacy rights and consumer protection for residents of California, United States.

The CCPA becomes effective on January 1, 2020.