Capgemini

California Consumer Privacy Act versus General Data Protection Regulation

How to make your business compliant

Data breaches are on the rise. While retail remains the most-targeted sector, incidents exposing personal data and billing information can happen in any industry.

Governments are introducing new rules and regulations to help protect consumers and enforce reporting. In May 2018, the European Union introduced the General Data Protection Regulation (GDPR), designed to put the consumer in control of their personal data, with significant fines for non-compliance and strict reporting requirements.

GDPR was unique because it moved the onus of proving consent to businesses collecting data on EU citizens and introduced significant fines for non-compliance. It was also seen as the future of consent and protection of consumer data. It was expected others would follow.

California did just that, enacting the California Consumer Privacy Act (CCPA) in June 2018. It takes effect on January 1, 2020, and may be the most extensive consumer privacy law in the country.

Like GDPR, the CCPA provides a new set of digital rights that puts the consumer in control of their personal data. The CCPA is meant to encourage transparency and ensure businesses properly inform consumers about how they use their information and if they experience a data breach. It also defines data processing and encourages businesses to be more accountable for the information collected on their customers.

California's very large economy — greater than that of the UK, for example — means the CCPA penalties may be even more significant than those imposed by the GDPR.

How you can prepare

CCPA compliance starts with an assessment of your data privacy maturity and examining its impact on your business operations. It is more than just managing a database. It is developing an overall privacy program that matches a company's specific needs, appetite for risk, and organizational structures.

Your CCPA journey needs a partner you can trust to manage the entire lifecycle. To learn more about how we can help, please see Preparing for the CCPA

Here is how the regulations compare:

	CCPA	GDPR
Start date	January 1, 2020	May 25, 2018
Definitions	Protected: “Consumer” Protector: “Business”	Protected: “Data subject” Protector: “Data controller”
Consumers	California residents	EU citizens
Companies affected	Any company doing business in California that: • Generates more than $25 million annual revenue • Processes personal data on 50,000-plus consumers, households, or devices • Derives 50%-plus of annual revenue selling personal data	Any company processing data on EU citizens
Personal data definition	• Data that identifies, relates to, describes, is capable of being associated with, or could be directly or indirectly linked with a particular consumer or household • This could include browsing history and behavioral data	• Expanded definition of personal data • Can include photos, medical records, financial status, fingerprints, banking details, and social-media posts • Applies to both structured and unstructured data, so it affects more than traditional databases
What it means for consumers	• Opt out of data collection. (Under age 16 must opt in before data collection occurs) • Know what data is collected • Request a copy of data • Request deletion of any data collected as of January 1, 2019 • Right to non-discrimination	• Opt in before data collection occurs • Know what data is collected • Request a copy of data • Request deletion of data • Right to restrict processing • Right to object • Right to data portability
Consent	• Can be established if a consumer signs up or makes an online purchase • Only offers consumers the right to opt-out	• Companies are required to secure consent from consumers via opt-in before collecting data
Response time	• Response within 30 days for a consumer request	• Response within 40 days for a consumer request
Penalties	• Unintentional breach: $2,500 per incident • Intentional breach: $7,500 per incident • Damages: $100 to $750-plus per consumer per incident	Fines: Up to the greater of €20 million or 4% of annual revenue

About Capgemini

A global leader in consulting, technology services and digital transformation, Capgemini is at the forefront of innovation to address the entire breadth of clients' opportunities in the evolving world of cloud, digital and platforms. Building on its strong 50-year heritage and deep industry-specific expertise, Capgemini enables organizations to realize their business ambitions through an array of services from strategy to operations. Capgemini is driven by the conviction that the business value of technology comes from and through people. It is a multicultural company of 200,000 team members in over 40 countries. The Group reported 2017 global revenues of EUR 12.8 billion (about $14.4 billion USD at 2017 average rate).

Learn more about us at

www.capgemini.com

For more details contact:

Alex Redlich
Privacy Practice Leader, Insights & Data
alex.redlich@capgemini.com

Prasad Lanka
Privacy Engagement Manager, Insights & Data
prasad.lanka@capgemini.com

People matter, results count.