California Consumer Privacy Act (CCPA) delivers a data opportunity

Enhanced privacy and security builds brand reputation and customer loyalty

Data breaches cost more than just money. Leakage of customer data and information is particularly damaging to a company's brand and reputation. Despite several years of trust building, one significant data incident quickly erases those gains, especially if there is a perceived delay in reporting the incident.

Since the EU enacted the General Data Protection Regulation (GDPR), 39% of consumers have increased their spending by as much as 24% with companies that protect their personal data, according to the Capgemini Research Institute. In addition, 39% have purchased more products and increased their spend, with more trust in their security. And 49% say they share positive experiences with friends and family.

Consumers are quick to relinquish brand loyalty when they believe their data protection is not a key priority. The same research showed 75% would ask to delete their data and more than 70% would reduce spending or switch to a competitor.

Data security is a key part of your brand affinity; keeping your customer's data secured is a priority to not only build trust, but loyalty.

GDPR inspires more privacy legislation

Governments are moving to tighten privacy laws. As expected, the GDPR, introduced by the EU in May 2018, has led other countries such as Canada, Japan, and India to review their data privacy laws.

California is the first US state to strengthen these laws. The California Consumer Privacy Act (CCPA) goes into effect on January 1, 2020, but businesses need to be prepared before the deadline date. The new legislation will apply to any consumer data collected in the 12 preceding months, so if you collect consumer data from January 1, 2019, a consumer may ask for the data to be deleted a year later, and the business must comply.

Similar to the GDPR, the CCPA gives more control to the consumer on how their data is collected, used, and deleted. Businesses must prepare for an influx of inquiries and requests that require swift action.

What is the CCPA?

CCPA applies to companies that conduct business in the state of California or collect or process personal information about California residents. It applies to business that meet at least one of the following criteria:

- Generates gross annual revenue of more than $25 million
- Buys or shares personal information about 50,000 or more consumers, households, or devices
- Derives at least one-half of its annual revenue from selling consumers' personal information

GDPR expanded the definition of data that are personal identifiers, and the CCPA follows this lead. Consumer information is more than just a simple name or address. Under the CCPA, personal data could include postal address, email address, Internet protocol (IP) address, driver's license number, social security number, browsing habits, and behavioral data.

Capgemini recently worked with a client to create data lineage across 400 separate business processes.

Significant penalties for non-compliance

Under CCPA, the state will impose fines of $2,500 per incident for unintentional breaches and $7,500 per incident for intentional violations. It also allows consumers to recover up to $750 per incident, or more if the consumer can show actual damages that exceed $750. The amounts might seem modest, but CPPA penalties have the potential to be substantial, especially if the CCPA decides on a per-consumer per-incident model. So, if you expose personal data on one million consumers, your business could be required to pay damages of at least $750 million, in addition to any possible legal action pursued by affected individuals.

Assessing CCPA readiness

Many CCPA requirements are not new, however the act is an opportunity to review and improve existing data-security strategies, privacy policies, and statements. Companies need to understand how they collect, process, access, and transmit data, and ensure they comply with CCPA standards.

If your company maintains consumer data across multiple lines of businesses and databases, you will need to:

- Be able to access all instances of consumer data in all your locations if a consumer asks for it
- Create audit trails to prove you have complied with a consumer data deletion request
- Identify data that cannot be deleted for a specified period of time due to industry regulations such as finance, insurance, healthcare, and real estate.

The CCPA will require new capabilities for managing consumer inquiries. A company will need multiple channels to receive consumer, the ability to uniquely identify a consumer, to make data available in a portable format, to make exceptions for data that needs to be retained, and resolve disputes.

Delivering CCPA compliance

Capgemini knows security fundamentals and digital, data-driven strategies. The CCPA requires businesses to use only the data needed for a given task and seek consent before using data for a different task.

Our powerful and flexible end-to-end solution matches your specific needs, appetite for risk, and organizational structures. We combine data management and security services to discover, classify, and clean up data. The byproduct of applying appropriate controls to private data is the clean-up of the overall operating environment and removal of significant amounts of non-used data and duplicate databases. In addition, strategies may include an approach that pseudonymizing private data for analytics purposes, so businesses can still leverage customer data to make decisions.

Our overall privacy program approach includes policy, controls, architecture (Privacy by Design), and compliance management, and ensures all aspects of data response and management are performed properly. Our privacy governance and Privacy by Design supports the application lifecycle. It also provides IoT and data-usage transparency that is built into applications and backend systems to ease overall privacy governance requirements.

Every business manages lifecycles for data. Privacy by Design means that data privacy is built into these processes, rather than added later. Companies which must comply with CCPA need to assess any application that collects consumer data.

Capgemini recommends a data privacy framework built on five core elements:

Governance: From data classification to executive-level metrics, data privacy begins and ends with governance.

Policy: A data privacy policy enables you to identify gaps when new regulations emerge and establish the road map to remediation.

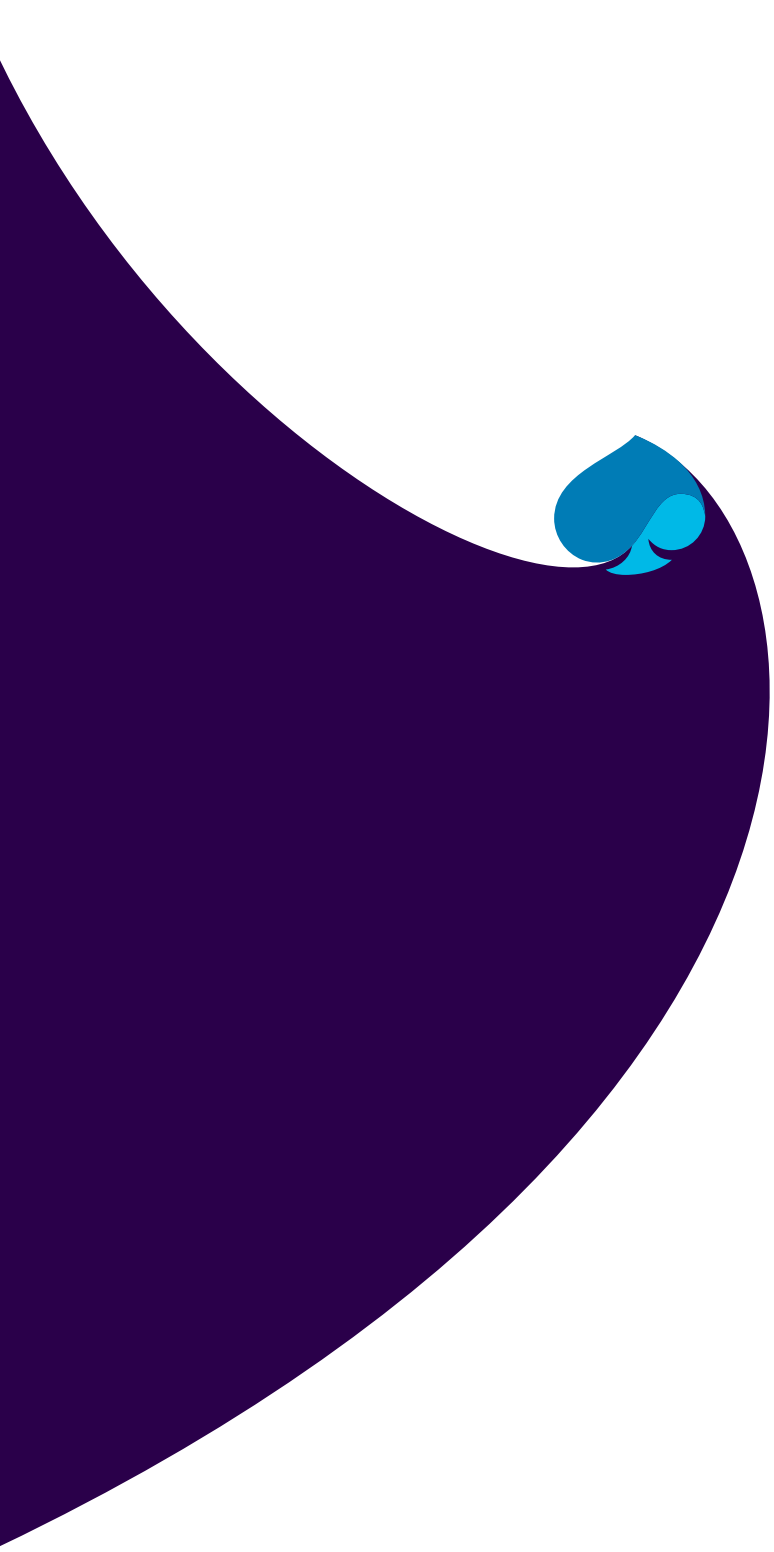
Process: Process is where the policy rubber meets the road. It's your mechanism for closing gaps and achieving compliance.

Awareness: Training and ongoing communication are essential to making sure a data privacy mindset extends throughout your enterprise.

Technology: From firewalls to encryption, from vulnerability assessment to patch management, security technology and IT processes are crucial to data protection.

Following a proven, phased approach, you can rapidly and effectively achieve CCPA compliance and at the same time collect and use consumer information to contribute to your business goals. You want a partner you can trust to manage the entire lifecycle of your CCPA journey.

To learn more about how we can help, please see Preparing for the CCPA



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.