sia partners

INSIGHT

NOVEMBER 2018

CALIFORNIA CONSUMER PRIVACY ACT:

THE AMERICAN GDPR?

Driven by the continued global rise in consumer data breaches and growing privacy concerns, the State of California recently passed the California Consumer Privacy Act of 2018 ("CCPA"). The CCPA represents the most demanding customer data privacy statute enacted to date at the U.S. state level. Businesses like financial institutions will need to consider existing privacy rules in the U.S. when assessing the potential impact of CCPA.

The CCPA is similar to the recent European Union's General Data Protection Regulation ("GDPR") that came into effect in May 2018. While CCPA and GDPR have differences, both laws provide consumers a greater ability to control their personal information. The CCPA also imposes requirements and prohibitions on businesses that collect or sell this information.

Although the CCPA became California state law on September 23, 2018, the Attorney General's enforcement of the CCPA goes into effect six months after publication of the implementing regulations, or July 1, 2020, whichever comes first. Sia Partners will continue to monitor and report on regulations issued by the Attorney General of California.

This article contains what we know about the CCPA now.

What is the CCPA?

The CCPA is designed to protect California residents' personal information from the threats of unwanted disclosure, sharing or sale. A key objective of the CCPA is to prevent situations like the recent event involving Cambridge Analytica gaining access to personal information of approximately 87 million Facebook users without their consent.

The CCPA defines personal information as the 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. Personal information includes, but is not limited to, name, address, social security number, passport or driver's license number, biometric, geolocation, education and internet activity information including web browsing history. Personal information can be collected actively through contracts or passively through cookies and IP addresses.

The CCPA gives California residents a set of new privacy rights:

Privacy Rights	Description
1. Right to Know	The right of Californians to know (a) what personal information is being collected about them and (b) whether their personal information is sold or disclosed and to whom.
2. Right to Access	The right of Californians to access their personal information held by businesses or their third parties.
3. Right to Request Deletion	The right of Californians to request businesses to delete their personal information, subject to certain exceptions like the need for the business to comply with legal obligations.
4. Right to Opt Out, Opt In	The right of Californians to prohibit the sale of their personal information ("opt-out") and the need to authorize such a sale for individuals 16 years-old or younger ("opt-in").
5. Right to Equal Service and Price	The right of Californians to not be discriminated against when exercising their privacy rights.
6. Right to Seek Damages	The right of Californians to seek statutory damages from businesses in case of violations. Statutory damages range from $100 to $750 per consumer per incident or actual damages, whichever is greater.

A consumer may bring an action under the CCPA only for an alleged business failure to "implement and maintain reasonable security procedures and practices" that results in a data breach. To help enforce these rights, the CCPA imposes requirements and prohibitions on businesses that collect or sell personal information:

Business Requirements and Prohibitions	Description
1. Disclosure Requirements	Upon receipt of a verifiable consumer request, businesses will be required to disclose: 1) The categories and specific pieces of information that they collect about the consumer; 2) The categories of sources from which that information is collected; 3) The business purposes for collecting or selling the information; and 4) Categories and identify of third parties with which the information is shared.

2. Deletion Requirements	Upon receipt of a verifiable consumer request, businesses will be required to delete the personal information as long as it does not interfere with the legal obligations of the business.
3. Opt-out Requirements	Businesses will be required to grant a consumer's verified request to opt-out from the sale of their personal information.
4. Opt-in Requirements	Business will be required to seek affirmative authorization for selling the personal information of consumers under 16 years of age.
5. Discrimination Prohibition	Businesses will be prohibited from discriminating against customers who exercise their personal information-related privacy rights. Businesses will have the ability to offer financial incentives for the collection of personal information.

Does CCPA Apply To Your Business?

The CCPA impacts businesses, independent of where their operations are located, that collect, share or sell personal information of California residents. These individuals could be consumers as well as employees or independent contractors. According to experts in a recent article published on Bloomberg BNA, the CCPA will apply to over 500,000 businesses servicing approximately 40 million California residents.

The CCPA also lists a number of **exemptions** that need to be considered when determining a business's applicability to the act. These exemptions relate to existing U.S. privacy laws. Subject to certain exemptions discussed below, the following decision tree outlines the initial determination whether CCPA will impact a business:

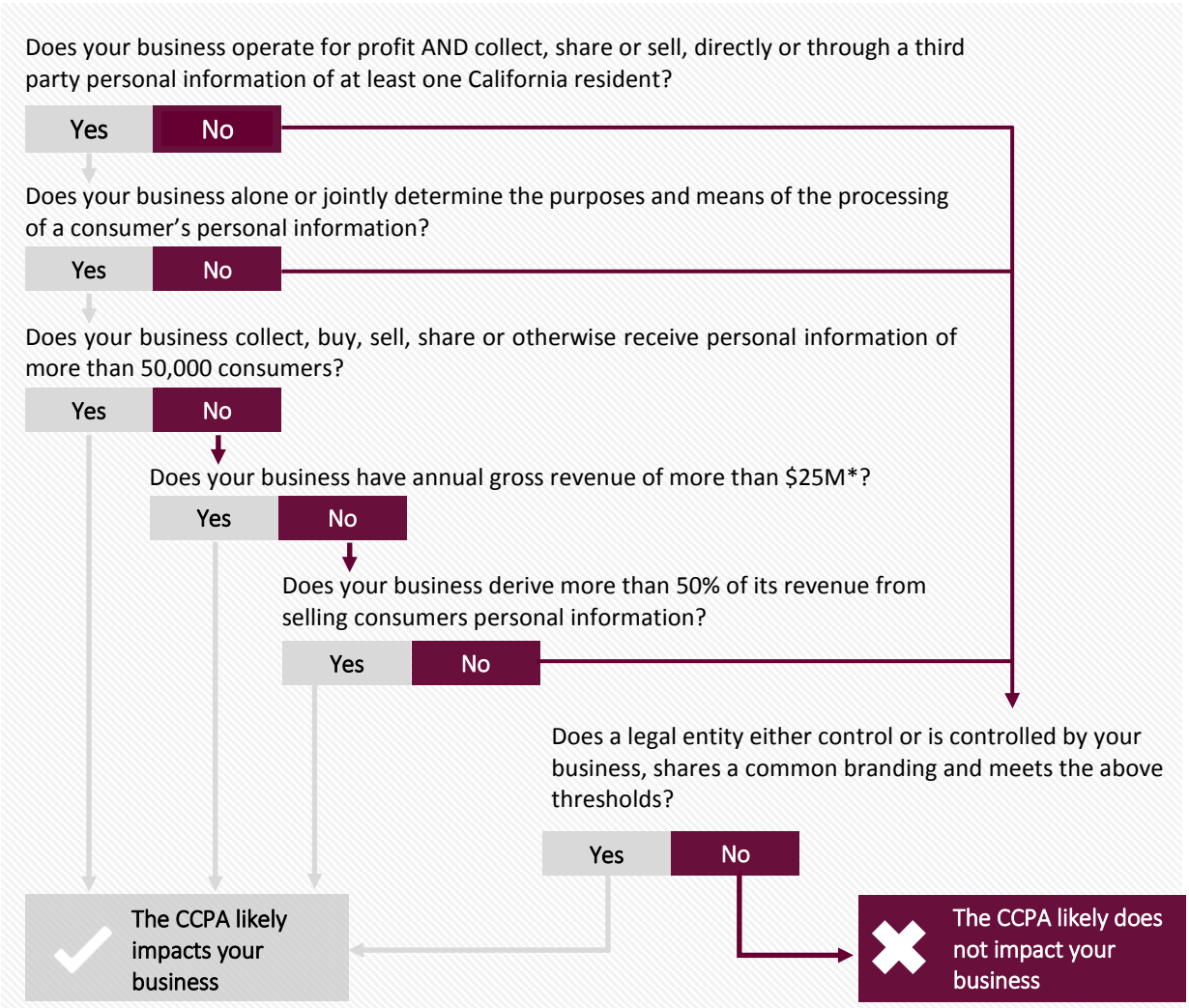


FIGURE 1: CCPA ENTITY COVERAGE DECISION TREE

* Currently, the CCPA does not specify whether the $25M threshold represents annual gross revenue worldwide or for only California, so further clarification is needed

>> CCPA exemptions

Even though a business may appear to be covered under the CCPA, there are a number of exemptions that limit the act's applicability. The CCPA does not apply to some personal information collected, sold or shared by covered entities governed by the Confidentiality of Medical Information Act ("CMIA"), the Health Insurance Portability and Availability Act ("HIPAA"), the "Common Rule" or the California Financial Information Privacy Act ("CFIPA"). In addition, the CCPA exempts health care providers to the extent that they maintain "patient information" in the same manner as medical information or protected health information governed by the HIPAA or the CMIA.

Nonpublic information collected by financial institutions subject to the Gramm-Leach-Bliley Act ("GLBA") or the CFIPA, may not be subject to the CCPA. However, GLBA-regulated entities will likely remain subject to the private right to seek damages under the CCPA.

GLBA entities will likely remain subject to the provisions and requirements of the CCPA if they engage in activities falling outside of the GLBA—which they almost certainly will. To the extent that GLBA-regulated entities are using targeted online advertising, tracking web page visitors, and, or collecting geolocation data—to name a few examples—either through their web pages or apps, they will need to analyze the CCPA requirements.

Performing an analysis will help organizations determine the CCPA's applicability to their businesses. For instance, a financial institution governed by existing privacy laws, such as the GLBA, will likely have to comply with the CCPA's new privacy rights for the categories or specific pieces of personal information that are not already covered by existing U.S. privacy laws

CCPA to GDPR Comparison

Both the CCPA and GDPR define personal information in similar ways with respect to privacy rights and enforcement mechanisms. While both regulations have similarities, compliance with one will not guarantee compliance with the other.

Key similarities include:

- **Privacy rights** - set the privacy of personal information as a fundamental right.
- **Transparency** - improve transparency and communication about the personal information being collected or sold and the purposes of its use.
- **Policies** - require establishing sound data privacy policy and procedures.
- **Penalties** - impose penalties and fines.

Key differences include:

- **Governance** - GPDR explicitly requires organizations to establish a data governance framework while the current CCPA bill does not explicitly mention such a requirement.
- **Consent collection** - the CCPA gives consumers the right to opt-out from the sale of personal information while GDPR requires businesses to collect consumer consents, "opt-in", if they want to collect, use, share or sell personal information for purposes other than indicated in the contract. The CCPA only requires businesses to collect consent, "opt-in", to sell personal information for consumers under 16 years old.
- **GDPR rights** - GDPR gives consumers the rights to request businesses to (1) rectify their personal information, (2) restrict the use of their personal information outside of contract processing, and (3) avoid using automated decision-making processes like profiling. The current CCPA bill does not include such provisions.
- **Access period** - the CCPA gives California residents the right to access their personal information collected during the last 12 months, while the GDPR does not have a time limitation for EU citizens to access their personal information.
- **Discrimination** - the CCPA prohibits businesses from discriminating against consumers who exercise their privacy rights while the GDPR does not.
- **Transfers** - GDPR allows businesses to transfer personal information of EU residents to any entity outside the EU under certain conditions while the current CCPA bill does not address territoriality.
- **Disclosure** - the CCPA requires businesses to (1) disclose its data privacy policy on its website and in public statements, and (2) display a link on their website's homepage for consumers to "opt-out" of the sale of

their personal information. GDPR only requires the policy disclosure.

What Businesses Need to Do

Businesses first need to assess the CCPA's applicability to their operations. Once the need to comply with some or all of CCPA sections is confirmed, businesses need to assess whether their existing data privacy and information security policies, procedures and practices are sufficient to meet the CCPA requirements.

Our experience working with clients to establish resilient and sustainable data privacy and information security capabilities that are compliant with regulatory expectations demonstrates that the effort can be organized across the following areas:

- **Governance** - identification, design, and roll out of stakeholders and oversight Committees.
- **Program management** - implementation plan development and execution, training, interaction with the business, oversight and control functions.
- **Data program** - data identification program to identify and understand personal information e.g., sources, purposes, flow, transfers, applications, security measures, third parties.
- **Legal, information, and transparency** - contract clause review, customer notification about the collection of additional data and about new purposes, management of client requests, reporting, disclosures on website.
- **Data security** - physical and IT security measures enforcement, collaboration with IT teams.
- **Policy, procedures and documentation** - policy and procedures gap, maturity assessment against regulatory expectations and market-leading practice and subsequent enhancement.

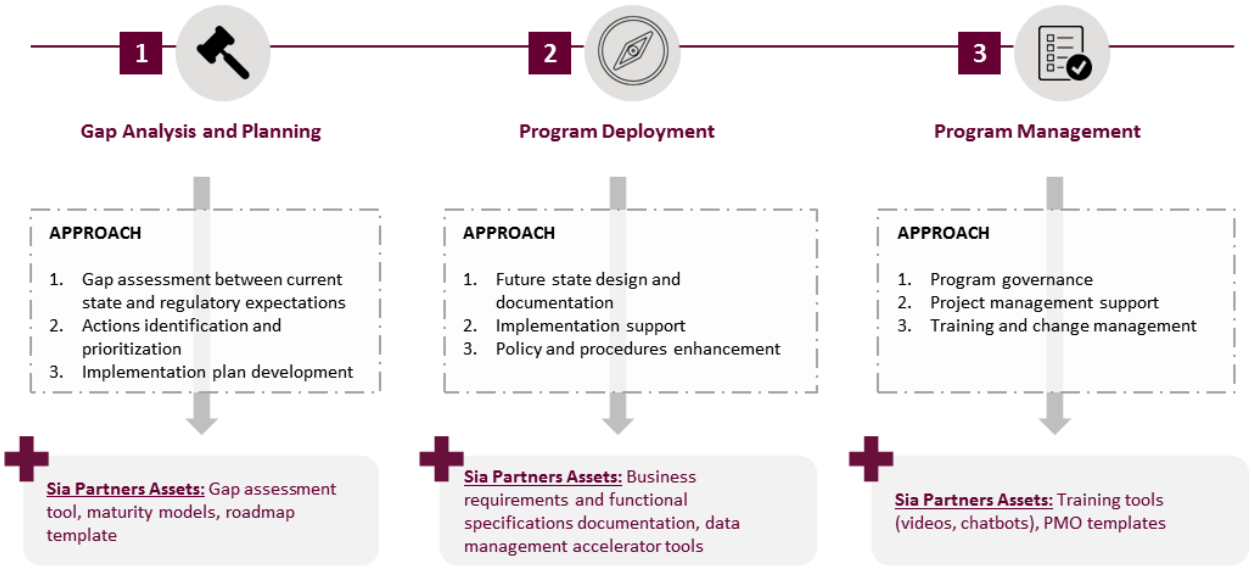
The success of the CCPA compliance project relies on an organization's ability to mobilize its workforce and create a long-term solution based on a sound corporate culture and effective governance.

As segmenting the population between California residents and other consumers could be a challenge, businesses should consider applying the CCPA to all U.S. consumers, employees, and contractors. Businesses may need to track CCPA-related changes as soon as 2019 so further clarification from the Attorney General's office related to the implementing regulation is needed.

How can Sia Partners help?

Sia Partners has developed documentation, templates, methodologies and tools e.g., gap assessment tool, to assist businesses with their initiatives to comply with the CCPA:

Sia Partners has completed more than 80 GDPR and other data privacy projects and can leverage this experience and our accelerator tools to support your CCPA initiatives.



YOUR CONTACTS

DANIEL H. CONNOR

CEO US
+ 1 (862) 596-0649
daniel.connor@sia-partners.com

DAVID GALLET

Associate Partner
+ 1 (347) 577-2063
david.gallet@sia-partners.com

LAUREN L. PICKETT

Director
+ 1 (917) 439-3328
lauren.pickett@sia-partners.com

EDWARD GUADIANA, J.D.

Sr. Consultant
+ 1 (646) 496-0160
edward.guadiana@sia-partners.com

CYRIL SAYADA

Sr. Consultant
+ 1 (929) 363-9791
cyril.sayada@sia-partners.com

LOÏC VACHON

Sr. Consultant
+ 1 (917) 442-3527
loic.vachon@sia-partners.com

ABOUT SIA PARTNERS

Sia Partners is a next generation consulting firm focused on delivering superior value and tangible results to its clients as they navigate the digital revolution. With over 1,200 consultants in 15 countries, we will generate an annual turnover of USD 230 million for the current fiscal year. Our global footprint and our expertise in more than 30 sectors and services allow us to accompany our clients worldwide. We guide their projects and initiatives in strategy, business transformation, IT & digital strategy, and Data Science. As the pioneer of Consulting 4.0, we develop consulting bots and we integrate the disruption of AI in our solutions.

Abu Dhabi
PO Box 54605
Al Gaith Tower #857
Abu Dhabi – UAE

Amsterdam
Barbara Strozzilaan 101
1083 HN Amsterdam - Netherlands

Brussels
Av Henri Jasparlaan, 128
1060 Brussels - Belgium

Casablanca
46, Boulevard Adbellatif Ben Kaddour, Racine – Casablanca 20000 - Morocco

Charlotte
101 S. Tryon Street, 27th Floor, Charlotte, NC 28280, USA

Doha
Al Fardan Office Tower #825
PO Box 31316
West Bay Doha - Qatar

Dubai
Shatha Tower office #2115
PO Box 502665
Dubai Media City
Dubai - UAE

Hong Kong
23/F, The Southland Building, 48 Connaught Road Central
Central - Hong Kong

Houston
800 Town and Country Boulevard, Suite 300
77024 Houston, TX

London
36-38 Hatton Garden
EC1N 8EB London - United Kingdom

Luxembourg
7 rue Robert Stumper
L-2557 Luxembourg

Lyon
3 rue du Président Carnot
69002 Lyon - France

Milan
Via Vincenzo Gioberti 8
20123 Milano - Italy

Montreal
304 - 19 Rue le Royer Ouest
Montreal, Quebec,
Canada, H2Y 1W4

New York
40 Rector Street, Suite 1111
New York, NY 10006 – USA

Paris
12 rue Magellan
75008 Paris - France

Riyadh
PO Box 91229
Office 8200 - 12, Izdihar city
Riyadh 11633 - KSA

Rome
Via Quattro Fontane 116
00184 Roma - Italy

Singapore
137 Street Market, 10-02
Grace Global Raffles
048943 Singapore

Tokyo
Level 20 Marunouchi Trust Tower-Main
1-8-3 Marunouchi, Chiyoda-ku
Tokyo 100-0005 Japan

For more information, visit: **www.sia-partners.com**

Follow us on **LinkedIn** and **Twitter @SiaPartners**

siapartners