California Privacy Act Vs. The General Data Protection Regulation

Organizations across the globe are making their way back to the 'war room' to analyze the applicability of one of the most comprehensive data privacy laws sweeping the US, the California Consumer Privacy Act of 2018 ("CaCPA") against their business processes. The CaCPA, approved on June 28, 2018, was designed to give consumers (i.e. Californians) control over the use, including the sale, of their personal information. This law conceptually, has similar characteristics to the European Union's data protection regulation, including its ability to be enforced on a global scale.

schellman
Quality. above all.

While both privacy acts share a similar intent, the CaCPA certainly has its own set of specific characteristics that sets it apart from its European counterpart, and although it appears that many of the general provisions appear to be borrowed from the GDPR and other global privacy practices, organizations will need to carefully evaluate the appropriateness of previously developed policies, procedures, or processes to meet California's new privacy provisions.

In this article, we look at the new CaCPA in comparison to the EU General Data Protection Regulation (GDPR). The aim is to help identify certain similarities and differences between the two regulations to help organizations better strategize their effort in achieving compliance with both.

Before you set out to solidify your compliance strategy, be sure to check on the latest developments issued by California to ensure that your understanding of the CaCPA remains consistent with the attorney general's guidance and expectations.

View California's Guidance and Expectations →

So, the big question is: **Can you rely on GDPR to satisfy the requirements of CaCPA?**

Simply put - no.

The CaCPA has its own set of explicit requirements needed for compliance. In a similar manner, compliance with CaCPA would not signify adherence to GDPR's requirements. We will touch on a few examples later in this article.

Planning for similarities and differences among the privacy laws

When approaching the new CaCPA, organizations should consider their current processes designed for meeting existing privacy obligations, such as local, national, and international requirements (i.e. GDPR), and how those processes could reasonably apply to CaCPA based on a comparative risk assessment. Foundations laid out by these privacy requirements will play a beneficial role in the adoption of the new requirements. Additionally, other California privacy-oriented laws, may provide useful strategic information, including the following:

- Online Privacy Protection Act of 2003 (Cal. Bus. & Prof. Code § 22575)
- Information Security Statute (Cal. Civ. Code § 1798.81.5)
- Data Breach Notification Statute (Cal. Civ. Code § 1798.82)
- Disposal of Customer Records (Cal. Civ. Code § 1798.81)

Nevertheless, changes to automated and manual processes will likely be required in pursuit of a CaCPA-compliant operation. There are overlapping requirements among the laws; however, those should be carefully considered for coverage, as they may not be a 1-to-1 match. Particularly, in cases where the requirements in one framework is more lenient than the other; the response requirements could be confusing and potentially conflict with the rights afforded to an individual in a particular jurisdiction; for example:

- Inquiry Response Time: CaCPA's 45-day time period v. GDPR's undue delay/30-day max
- Consent: CaCPA's opt-out requirement v.GDPR's opt-in/consent requirement
- Privacy Notice: CaCPA's annual update requirement v. GDPR's undefined time period

Example Similarities and Differences among the CaCPA and GDPR

As noted, general commonalities may exist among the regulations but require a detailed inspection to accommodate for the minor variances detailed under each program.

Determining an organizations applicability

CaCPA Clause	GDPR Article	Implications
For-profit organizations doing business in California and meets one or more of the following criteria: 1. Annual gross revenue > $25mm 2. Buys, receives, sells, or shares PII of 50,000 or more consumers on an annual basis 3. Derives 50% or more of revenue from personal information sales	Organizations processing personal data transferred from EU member states (as a Controller or Processor)	• These parameters are circumstantially different; both apply under certain conditions and are based on the type and nature of data collected, processed, or disclosed to third-parties.
Refer to: 1798.120(a)	**Refer to:** Article 3 and Article 4a	

Classification of personal data

CaCPA Clause	GDPR Article	Implications
In a broader manner, the CaCPA governs the processing of California consumers personal data. However, this also covers employment education, medical, and children's data; and, information that can identify a 'household' rather than an individual.	The GDPR governs the processing of personal data transferred out of the EU. This includes standard personal data fields as well as special categories (i.e. sensitive data).	• Although similar in nature, the CaCPA provides more extensive coverage on the personal data definition; including the classification of 'household' information. Conceptually comparable in the sense that organizations should be concerned with identification of an individual or determine that the data can effectively be used to identify an individual. • 'Household' data has not yet been explicitly defined under the CaCPA; however, to some privacy professionals, it could include information such as: energy and resource consumption of a household, IP addresses and online identifiers, property records, web browsing history and associated online behaviors.
Refer to: 1798.140(o)(1)	**Refer to:** Article 4(1) and Article 9	

Privacy Notice criteria

CaCPA Clause	GDPR Article	Implications
The CaCPA requires organizations to update their privacy notice every 12 months.	The GDPR expects organizations to maintain an accurate privacy notice to inform individuals of the processing activities performed by the organization. However, annual updates to the notice are not required.	• The requirements for the CaCPA are stricter than the GDPR and requires annual visitations to the public facing privacy notice. • The GDPR does not specify review periods for the privacy notice.
Refer to: 1798.130(a)(5)(a)	**Refer to:** Article 5 and Articles 13-14	

Opt-in, Opt-out, and Consent

CaCPA Clause	GDPR Article	Implications
Different from the GDPR, organizations must only provide individuals with the ability to opt-out of sales that include the consumers personal information without requiring their consent to initiate the sharing.	Stricter than the CaCPA, organizations, under certain conditions, would need an individual's consent (i.e. opt-in) to activities involving data collection, processing, or disclosure of personal information to a third party. Similar to the CaCPA, the GDPR also requires an organization to permit individuals to revoke consent that was previously provided.	• The requirements for CaCPA and GDPR are different with respect to opt-in and opt-out. CACPA requires organizations to respect an individuals' request to opt-out of certain data sharing arrangements. • Different from the GDPR, the CACPA does not require previously provided consent to initiate data sharing with third parties.
Refer to: 1798.120(a)	**Refer to:** Article 7	

Required contact methods to reach the organization

CaCPA Clause	GDPR Article	Implications
Stricter than the GDPR, organizations must make available to consumers two or more designated methods for submitting requests for information required to be disclosed.	Having less defined requirements than the CACPA, organizations must only publish, within its privacy notice, the identity and the contact details of the controller and, where applicable, of the controller's representative.	Different from the GDPR, CaCPA requires at least two contact methods, including a telephone number and a website address to allow a user to contact the organization with any questions or requests.
Refer to: 1798.130. (a)(1)	**Refer to:** Article 13	

Employee Training

CaCPA Clause	GDPR Article	Implications
More specific than the GDPR, the CaCPA requires that all individuals responsible for handling consumer inquiries about the business's privacy practices or the business's compliance with this title are knowledgeable on the topics and how to direct consumers to exercise their rights under those sections.	Less specific than the CaCPA, the GDPR does not explicitly stipulate any training requirements; however, the DPO (where appointed) is required to engage in awareness-raising and training programs.	Different from the GDPR, the CaCPA explicitly states that employees must be knowledgeable of specific sections under the Act and to be capable of facilitating inquiries related to privacy.
Refer to: 1798.130(a)(6), .135(a)(3)	**Refer to:** Article 39	

Data collection limitation principles

CaCPA Clause	GDPR Article	Implications
Similar to the GDPR, organizations are obligated to collect specific sets of information, and only that which has been previously communicated to the user via a privacy notice.	Similar to the CaCPA, GDPR requires organizations to be transparent with their data collection activities; and, to only collect the minimum amount of data necessary to perform the processing activities.	Both frameworks have a similar approach in their requirements to be transparent (i.e. privacy notice) in its data collection activities; and, have specific purposes pertaining to the collection of key data fields.
Refer to: 1798.100(b)	**Refer to:** Article 5 and Article 25	

Responding to consumer requests

CaCPA Clause	GDPR Article	Implications
Less strict than the GDPR, organizations are required to respond to requests within 45 days.	Stricter than the CaCPA, the GDPR requires organizations are required to respond to requests without undue delay, but no later than 30 days.	The GDPR has a stricter turnaround time than the CACPA; organizations must be prepared to respect those timeframes accordingly, based on the context of the request, to abide by the applicable regulation. Organizations may decide to standardize processes based on the strictest (30 day) period.
Refer to: 1798.130. (a)(2)	**Refer to:** Article 12	

A users' right to equal service and price

CaCPA Clause	GDPR Article	Implications
Different from the GDPR, organizations are forbidden to discriminate against an individual in cases where they exercise the rights afforded to them under the CaCPA.	No relatable Articles under the GDPR	• The GDPR does not specify the right to fair and equal service in cases where a user exercises their rights under the Regulation. • The GDPR does include provisions around data portability and the requirements to not delete the data after this request has been exercised.
Refer to: 1798.125(a)(1)	**Refer to:** Not Applicable	

Data Accessibility

CaCPA Clause	GDPR Article	Implications
Similar to the GDPR, individuals have the right to request that a business that collects a consumer's personal information disclose to that consumer the categories and specific pieces of personal information the business has collected.	Similar to the CaCPA, the GDPR provides individuals with the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed.	• The accessibility rights between the two frameworks share similar characteristics, organizations should be prepared to classify the types and categories of data collected and processed about an individual. • Differences do exist in the CaCPA's requirement to communicate the specific pieces of personal information the business has collected about the consumer. This is not a requirement within the GDPR.
Refer to: 1798.100(a)	**Refer to:** Article 15	

Data Portability

CaCPA Clause	GDPR Article	Implications
Similar to the GDPR, individuals have the right to obtain a copy of their personal information in a portable and readily useable format that allows the consumer to transmit this information to another entity without hindrance.	Individuals have the right to obtain a copy of their personal information held by the organization; and, request a copy to be transferred to another organization.	• The data portability requirement is similar between the frameworks. Organizations should have processes in place to extract and export personal data fields associated to the individual. • The CaCPA obligates an organization to share a copy of personal data with a verified requestor; however, it does not require an organization to port data directly to another organization.
Refer to: 1798.100(d)	**Refer to:** Article 20	

Data Deletion

CaCPA Clause	GDPR Article	Implications
Similar to the GDPR, organizations must delete the consumer's personal information from its records and direct any service providers to delete the consumer's personal information from their records.	Organizations must delete personal information, as requested by the individual, and communicate the deletion requirement to sub-processors where the organization disclosed personal information to third parties.	The data deletion requirements are similar between the frameworks. Both require the personal data to be deleted from the organizations internal systems; and, communicate those deletion requests to third parties where PII has been shared.
Refer to: 1798.105(a)	**Refer to:** Article 17 and Article 19	

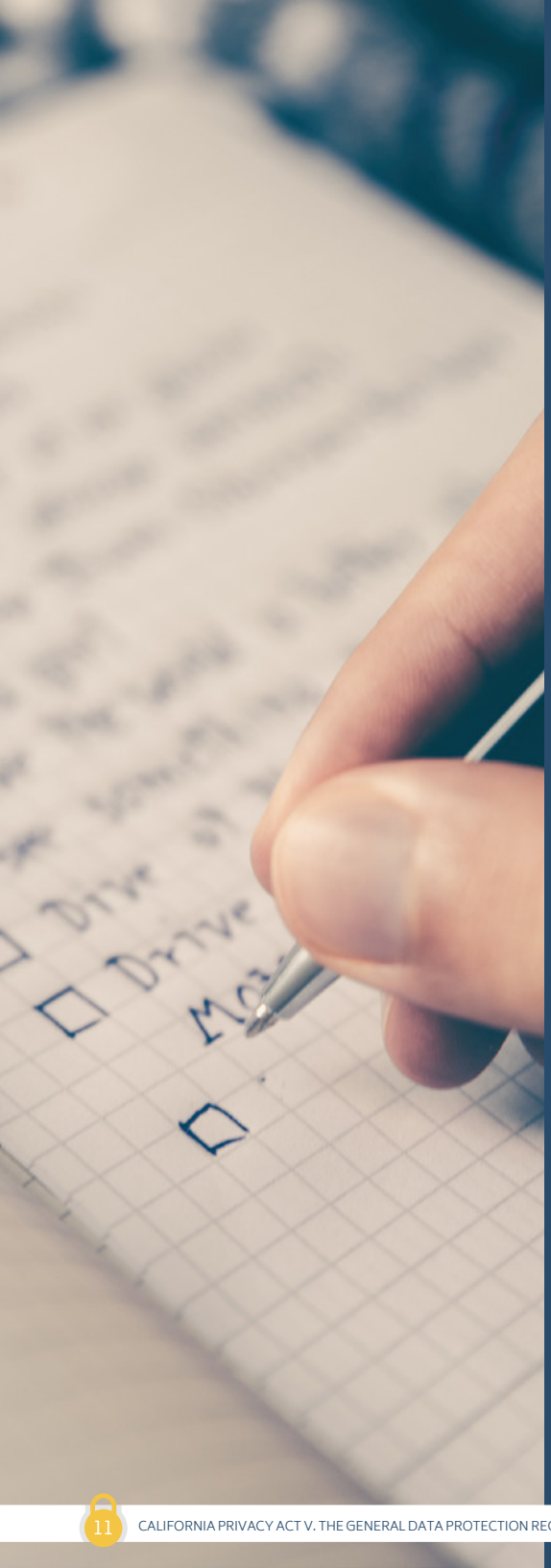
Plan to Act

The CaCPA is due to be enforceable on January 1, 2020.

It's very likely that you'll have deficiencies within your existing privacy governance program due to CaCPA's new requirements; therefore, the sooner you plan your strategy, undoubtably, the better off you'll be in assuring users, customers, and business partners in your preparedness.

In the interim, this cooling period prior to the 2020 deadline allows for changes and clarifications to the CaCPA and some of its unclear provisions. However, organizations should not delay their plans to:

- ✓ Assess readiness
- ✓ Identify gaps
- ✓ Perform risk assessments, and
- ✓ Remediate their deficiencies well before the go-live date.



Drafting your plan for compliance

In preparation for compliance, organizations will need to consider developing their CaCPA strategy to begin tackling the important elements of the law.

- ☐ Performing an assessment of risks to the unauthorized disclosure of personally identifiable information, and the related compliance requirements.
- ☐ Conducting a comprehensive data mapping / inventory to identify if California resident's data is collected or processed by the organization;
- ☐ Reviewing and revising internal policies and procedures based on new information classification definitions, third-party management standards, and access request processes;
- ☐ Ensuring appropriate opt-out mechanisms are in place for restricting the sale of a consumer's personal data;
- ☐ Reviewing the existing privacy notice to ensure that key fields stipulated under the CaCPA are communicated to users;
- ☐ Evaluating the need for age-validation measures and appropriate opt-in strategies for ensuring that underage California consumers (or their parents) under the age of 16 have agreed to data sales involving their information;
- ☐ Preparing for the rights to access, delete, and transfer a consumer's information at their request;
- ☐ Verifying that third-party contracts are up to date to respond to data deletion requests


schellman