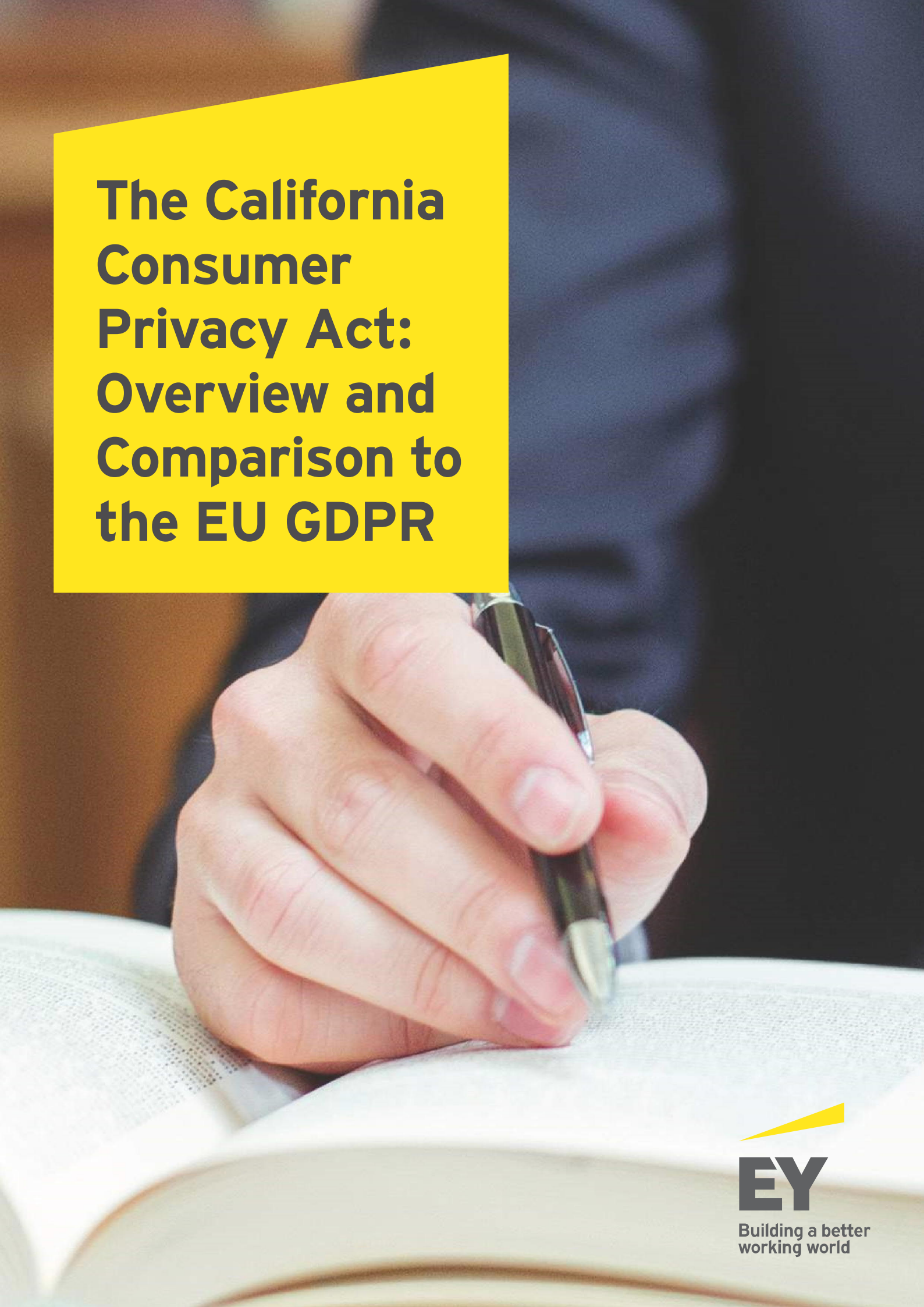

The California Consumer Privacy Act: Overview and Comparison to the EU GDPR

EY
Building a better working world

Introduction

During the months preceding the European Union's General Data Protection Regulation (GDPR) go-live, which occurred on 25 May 2018, California lawmakers were working on privacy legislation of their own. Initially, California activists intended to pass a privacy bill through the California ballot initiative process in the November 2018 election. However, this effort was abandoned when on 28 June 2018, Assembly Bill No. 375 (AB 375), which guarantees California residents rights around access, erasure, portability and opt-out, was signed into law, creating the California Consumer Privacy Act of 2018 (CCPA, or the Act). The Act was consciously designed to emulate certain provisions of the GDPR and does so by providing California residents many of the same rights for their personal data as are offered by the GDPR.

The enforcement date of the Act is 1 January 2020, and it is currently the broadest privacy law on the books here in the United States, requiring businesses that were previously exempt from the GDPR to spend the next 17 months redesigning the way they collect, process, share and retain data. It also represents what is predicted to be a trend across other states, which may ultimately result in all US. businesses evaluating their privacy programs.

Notably, the Act exempts personal information that is subject to the Health Insurance Portability and Accountability Act (HIPAA), as well as the sale of personal information subject to the Fair Credit Reporting Act (FCRA). Furthermore, personal information collected, processed, sold or disclosed pursuant to both the Gramm-Leach-Bliley Act (GLBA) and the Drivers Privacy Protection Act (DPPA) is also exempt, but only insofar as the CCPA is in conflict with those laws.

Companies will be limited in their ability to avail themselves of these potential exemptions unless they maintain a robust inventory of their business processes involving personal data, including detailed information about which data is subject to these other federal privacy laws. Financial institutions that are subject to GLBA and other companies subject to the DPPA may find it difficult to create a defensible argument that the CCPA is in conflict with these other laws, as the CCPA imposes new obligations not currently embodied in these other federal laws (e.g., the right to data deletion, opt-out of sale).

While working toward compliance with CCPA, companies can also use this opportunity to gain a competitive advantage by examining what needs to change and how data can be maximized within the confines of the trending requirements.

Who must comply with the Act?

The Act will apply to companies that:

1. Receive personal data from California residents and
2. Exceed — or their parent or subsidiary exceeds — one of three thresholds:
   a. Annual gross revenues of at least $25m;
   b. Obtain personal information of at least 50,000 California residents, households or devices annually; or
   c. At least 50% of their annual revenue is from selling California residents' personal information

If a company falls into an above category, it will need to evaluate its data practices and amend noncompliant practices by 1 January 2020.

California residents:

The law protects California residents, defined as:

"(1) Every individual who is in the State for other than a temporary or transitory purpose, and

(2) Every individual who is domiciled in the State who is outside the State for a temporary or transitory purpose"

Definition of sale of information:

The Act purports to apply to companies that sell California residents' personal data. However, the definition of "sale" provided is very broad and will cover most companies that handle California residents' personal data:

- "Sell," "selling," "sale" or "sold," means selling, renting, releasing, disclosing, disseminating, making available, transferring or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration.

What does the Act require?

The Act provides consumers with the following rights:

- Right to access the personal data collected about them and any third parties with whom the information is shared
- Right to erasure of personal information
- Right to opt-out to the sale of personal information
- Right to equal service and price when any of the above rights are exercised

Businesses are required to designate and share at least two methods (one telephonic and one web-based) by which consumers may exercise the above rights.

Right to access and erasure: Upon receiving a request for access to or erasure of personal information the business has on a consumer, the business is first required to authenticate the requester. Where the request was authorized, the business will have 45 days from the receipt of the request to complete the request.

Where the request is for access, the business must provide the consumer with:

- The categories of personal information collected about that consumer
- The types of sources from which the personal information was collected
- Whether the personal information was sold to any third parties
- The purposes for which the personal information was collected and/or sold
- The categories of third parties with whom the personal information is shared
- The specific pieces of personal information it has collected about the specific consumer making the request

Note on data portability: Where the information in response to a consumer access request is provided electronically, the information must be provided in a portable manner that allows the consumer to easily share it.

Both access and erasure must be provided to the consumer at no cost.

Opt-out: Businesses are required to provide consumers with a method by which to opt out of the sale of their personal information to third parties. The business must alert any relevant third parties with whom the personal information was shared that the consumer has exercised his/her opt-out right and erase that data from their systems.

To the extent that a consumer may exercise this right, and if a company is selling or sending that data to a third party, it is imperative that the data flows to the third parties is clearly understood. In addition, significant contractual updates will likely need to be made to the receiver of sold data, requiring them to act affirmatively if the transmitting company sends them an opt-out request.

Provide notice: Businesses are required to provide the consumer with a notice prior to the collection of any personal information, which covers:

- The consumers rights under this Act
- The categories of personal information the business will collect
- The purpose for which the personal information will be used
- Whether the personal information will be sold to third parties

Additionally, businesses must post an online privacy policy, containing a more general description of the personal information the business collects and sells to third parties, as well as a link entitled "Do Not Sell My Information," which directs the consumer to an opt-out for the sale of personal information.

Personal information:

The definition of personal information under the Act emulates or could potentially be broader than the definition in the GDPR. Personal information is defined by the Act as "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."

Examples of personal information in the Act:

1. Identifiers (e.g., real name, alias, postal address, unique personal identifier, online identifier Internet Protocol address, email, account name, Social Security number, driver's license number)
2. Commercial information (e.g., records of personal property, products or services purchased, obtained or considered, or other purchasing or consuming histories or tendencies)
3. Biometric information
4. Internet or other electronic network activity information (e.g., browsing history, search history, information regarding a consumer's interaction with a web site)
5. Geolocation data
6. Audio, electronic, visual, thermal, olfactory or similar information
7. Professional or employment-related information
8. Education information (not publicly available)
9. Inferences drawn from the information above to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities and aptitudes
10. Probabilistic identifiers

Comparing to the GDPR

- Those familiar with the GDPR will note that the rights to individuals created by the Act mirror those in the GDPR. However, it is important to note that in some areas, the Act goes further, while in other areas the Act is less prescriptive. To help navigate the two regulations, a summary comparing the two is provided below:

Focus area	Act	GDPR	Comparison summary
Access and portability	Upon consumer request, the company must provide: ▸ The categories of personal information collected ▸ The categories of sources from which the personal information is collected ▸ The business or commercial purpose for collecting or selling the personal information ▸ The categories of third parties with whom the business shares personal information ▸ The specific pieces of personal information that the business has collected about the consumer The data must be provided in a portable format that "allows the consumer to transmit this information to another entity without hindrance."	Upon consumer request, data controllers must: ▸ Confirm if they process an individual's personal data ▸ Provide a copy of the data (in commonly used electronic form in many cases) ▸ Provide supporting explanatory materials Consumers can request that their data be provided to them in machine-readable format if the data in question is: ▸ Provided by the data subject to the controller ▸ Processed automatically ▸ Processed based on consent or fulfilment of a contract	The Act and the GDPR have similar obligations, with a slight difference in response time. While California requires a response within 45 days, the GDPR requires response within a month. Further, California only requires disclosure covering the prior 12-month period, while the GDPR has no such time period limitation.

Focus area	Act	GDPR	Comparison summary
Notice	Prior to or at the point of collection, the business must notify the consumer of: ▸ The categories of personal information to be collected ▸ The purposes for which that personal information is collected ▸ The consumer's rights under the Act (access, to be forgotten, opt-out, etc.) The company is required to maintain this notice on its website and update it annually.	The business must provide a notice to the consumer, with an emphasis on information related to the data collection, including: ▸ The identity and contact information of the company collecting the data ▸ The purposes and legal basis for collecting the data ▸ How long the data will be retained The notice must be easily accessible and written transparently, using clear and plain language.	The requirements are largely similar under the two regulations
Right to be forgotten	Upon consumer request, the company must delete any personal information about the consumer that the business collected from the consumer and direct any service providers to delete the consumer's information from their records.	The data subject may request the erasure of their personal data without undue delay and the controller is obligated to erase the data when one of six criteria is met. However, obligations on data controllers to erase personal data and inform third parties do not apply "to the extent that processing is necessary."	There are similar obligations and exceptions under the GDPR and the Act, except that California requires response within 45 days, while the GDPR requires response within a month.
Opt-out	Companies must provide consumers with the right to opt-out of the sale of their personal information. Minors under the age of 16 have the right to opt-in to the sale of their personal information.	Consumers must opt-in to the sale of their PI before a company may act. Consumers may revoke this consent at any time.	While the Act focuses on an opt-out regime, the GDPR requires an opt-in regime.
Non-discrimination	Companies may not discriminate against a consumer in price or in services/goods offered because a consumer exercised a right under the Act.	Companies must make sure that there is no discrimination as a part of any automated decision-making or profiling processes.	The GDPR's anti-discrimination requirements are limited to automated decision-making, whereas the Act focuses on differing services or prices provided based on the exercising of consumer rights.
Employee training	Companies must train employees who handle consumer inquiries on the requirements of the Act.	Companies must provide training for and obtain attestation to privacy requirements from all employees who process personal information.	The requirements are similar under the two regulations.

Focus area	Act	GDPR	Comparison summary
Cross-border data transfers	No restrictions on cross-border data transfers.	Cross-border transfers of personal data to a third country must be based on an adequacy decision or, another valid data transfer mechanism (e.g., Binding Corporate Rules, Contract Clauses and EU-US Privacy Shield).	The GDPR restricts cross-border data transfers. The CCPA has no such restrictions.
Third-party management	A contract containing certain provisions is required for transfers to service providers and third parties.	Contracts containing certain provisions are required for transfers to data processors.	Both require written contracts to transfer personal information to third parties. However, there are more required provisions under the GDPR than under the Act.

Who can bring an action?

In addition to regulatory enforcement, the Act provides for a private right of action for certain violations of the statute. Specifically, the private right of action is limited to violations involving "unauthorized access and exfiltration, theft or disclosure of a consumer's non-encrypted or non-redacted personal information." The Act imposes several limitations on private rights of action, including:

- A narrower definition of "personal information" for private rights of actions than the much broader definition the Act provides for personal information elsewhere
- Plaintiffs must provide the company with 30-day written notice requesting remediation of the violation before being permitted to file
- The California Attorney General must be notified of any intended action and provide approval for the action to go forward

What are the penalties if a company does not comply?

The California Attorney General's Office may order a company to pay penalties up to $7,500 per violation for any intentional violation of the statute. If a company unintentionally violates the statute and fails to rectify its actions within a 30-day notice, the Attorney General may fine that company $2,500 per violation. A consumer filing a private right of action may recover damages ranging from $100 to $750, per consumer per incident, and companies can expect large class actions representing all individuals affected by a major breach or other systematic violation under the Act.

Conclusion

The Act imposes numerous new requirements on companies with California customers that mirror those of Articles 15–19 of the GDPR. Companies that have not aligned their data practices to align with the GDPR will have the largest programmatic changes to make to meet the January 1, 2020 go-live date for the Act. However, as companies are beginning to think about what these requirements mean for them, it is important to note that the California legislature anticipates amending and clarifying the Act prior to go-live.

Contacts

Scott Margolis
Executive Director

Tampa, Florida
+1 813 204 6188
scott.margolis@ey.com

Angela Saverice-Rohan
Executive Director

Los Angeles, California
+1 213 977 3153
angela.savericerohan@ey.com

Stefanie Ash
Senior Manager

Iselin, New Jersey
+1 732 516 5007
stefanie.ash@ey.com

Severino "Dino" Landingin
Senior Manager

New York, New York
+1 609 532 1195
severino.landingin@ey.com

Michael Podemski
Senior Manager

Chicago, Illinois
+1 773 715 5870
michael.podemski@ey.com

Reese Solberg
Senior Manager

Seattle, Washington
+1 206 262 7156
reese.solberg@ey.com

Shirin Ebrahimi
Manager

Los Angeles, California
+1 213 977 5078
shirin.ebrahimi@ey.com

Contributing authors

Katy Isakovich **Michelle Lease** **Gail Krutov**

EY | Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

SCORE no. 010931-18Gbl
1808-2841370

ED None

ey.com