ONE FIRM WORLDWIDE

California Consumer Privacy Act Guide

JONES DAY®

TABLE OF CONTENTS

EXECUTIVE SUMMARY

On June 28, 2018, California enacted the California Consumer Privacy Act ("CCPA")—the result of a last-minute compromise between California lawmakers and consumer privacy activists intended to avoid a widely criticized data privacy ballot initiative. The law, which is scheduled to go into effect on January 1, 2020, was amended in September 2018 and is likely to be modified again prior to the effective date. In its current form, the CCPA articulates certain data privacy rights of California residents, seeks to protect those rights by imposing new obligations on companies doing business in California, and grants the California Attorney General broad authority to implement related regulations.

Specifically, the CCPA enumerates the following five rights of California consumers:

1. The right to know what consumer personal information is collected by businesses.
2. The right to know whether the personal information is sold or disclosed, and to whom such information is sold or disclosed.
3. The right to say no to the sale of personal information.
4. The right to access the personal information.
5. The right to equal service and price, even if privacy rights are invoked.

The key provisions of the law require companies to respond to certain consumer requests regarding the collection and sale of their personal information. Importantly, the CCPA also provides consumers with a private right of action and statutory damages, in the event that certain unencrypted or unredacted personal information is subject to an unauthorized access and exfiltration, theft, or disclosure, as the result of a company's failure to implement and maintain reasonable security procedures and practices. In addition, the statute gives the attorney general the power to impose substantial penalties for violations of the statute, even if those violations do not result in a data breach.

Our experience counseling clients regarding the European Union's General Data Protection Regulation ("GDPR") suggests that successful compliance starts with substantial planning, preparation, and action prior to a law's effective date. Despite the uncertainty concerning the final form of the CCPA, covered companies should begin preparing for compliance with the law's new legal framework.

This guide provides a brief overview of the CCPA's key provisions, as well as the important changes it will make to the current rights, obligations, and remedies under California data privacy law. In addition, each section of this guide sets out a short list of suggested

actions that companies can take now to begin preparing for the CCPA's new requirements—and these actions are compiled into a single list at the end of the handbook.

We expect that this guide will help you prepare for the CCPA, and we hope you find it to be a useful tool. Please contact any of the lawyers listed on pages 26 and 27 if you would like to receive further information.

SCOPE[1]

Overview

The CCPA regulates the collection, possession, and sale of consumers' personal information by businesses. It gives consumers more control over the personal information that companies collect, and provides consumers with a new remedy in the event of a data breach that results in the "unauthorized access and exfiltration, theft, or disclosure" of certain personal information. It also provides the attorney general with broad rule-making authority and the power to impose substantial penalties for violations.

What Businesses Are Covered by the CCPA?

The CCPA applies to companies doing business in California that collect consumers' personal information (directly or through a third party) and that satisfy at least one of the following requirements:

- The entity has at least $25 million in annual revenue; or
- The entity receives, buys, sells, or shares for commercial purposes, alone or in combination, personal information on at least 50,000 California consumers, households, or devices; or
- The entity derives more than half of its annual revenues from the sale of personal information.

In addition, any entity that controls or is controlled by a business as defined in the CCPA—and that shares common branding with the business (i.e., a shared name, servicemark, or trademark)—is also covered by the law. Companies do not need to be based in California or have a physical presence in the state to be subject to the CCPA.

What Businesses, Conduct, and Data Are Not Covered by the CCPA?

The CCPA does not apply to entities such as government agencies, non-profit businesses, or certain small businesses. The CCPA also does not apply to medical information governed by the California Confidentiality of Medical information Act, or protected health information collected by entities covered by the privacy rules issued by the Department of Health and Human Services pursuant to HIPAA, or the HITECH Act; nor does it apply to providers of health care or covered entities who maintain patient information in accordance with those laws. In addition, the CCPA does not apply to certain information collected during clinical trials or to the sale of personal information to or from consumer reporting agencies for use in a consumer report. Furthermore, data collected, processed, sold, or disclosed pursuant to the Gramm-Leach-Bliley Act, the Driver's Privacy Protection Act, and the California Financial Information Act are excluded from most of the provisions of the CCPA; only Section 1798.150—which governs the

[1]Cal. Civil Code §1798.140(c); §1798.145(a)(6); §1798.175.

private cause of action for data breaches affecting certain categories of personal information—applies to this data. Finally, the CCPA does not apply to the collection or sale of personal information if every aspect of that commercial conduct occurs entirely outside of California.

What Are Other Important Aspects of the CCPA's Scope?

The CCPA applies to the collection and sale of consumer personal information by businesses, irrespective of whether the personal information was collected electronically or over the Internet. To the extent that there is a conflict between or among provisions in the law, the provisions that afford the greatest protection for the rights of consumer privacy control under those circumstances.

Action Items

- ✓ Determine whether your company meets the $25 million annual revenue threshold.
- ✓ Assess your company's practices concerning the collection and use of personal information.
- ✓ Ascertain how the collection and use of personal information affects your revenues.

DEFINITION OF PERSONAL INFORMATION[2]

Overview

For most purposes, the CCPA adopts an expansive definition of personal information ("PI") that includes "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." This definition is broader than the one in the existing California data breach statute; importantly, however, the CCPA does not amend or affect that statute's definition of personal information. Furthermore, as described in the Enforcement, Remedies, and Data Breaches section of this handbook, the CCPA's private cause of action only applies to cases of data breaches affecting narrower categories of data.

The CCPA's definition of PI encompasses not only the data elements typically regarded as personal information in most data breach notification statutes (such as name and Social Security number), but also includes data such as physical characteristics, biometric information, online identifiers, and aspects of a consumer's Internet activity.

Highlights of CCPA's List of Data Elements That Constitute "Personal Information"

- Identifiers, such as a real name, alias, postal address, unique personal identifier, online identifier, IP address, email address, account name, Social Security number, driver's license number, passport number, or other similar identifiers;
- Characteristics of protected classifications under California or federal law;
- Commercial information, including records of personal property, products or services purchased, obtained or considered, or other purchasing or consuming histories or tendencies;
- Biometric information;
- Internet or other electronic network activity information, including, but not limited to: browsing history, search history, and information regarding a consumer's interaction with a website, application, or advertisement;
- Geolocation data;
- Audio, electronic, visual, thermal, olfactory, or similar information;
- Professional or employment-related information;
- Education information, defined as information that is not publicly available or personally identifiable, as defined in the Family Educational Rights and Privacy Act (20 U.S.C. §1232g, 34 C.F.R. Part 99);
- Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics,

[2] §1798.140(o); §1798.145(a)(5); §1798.140(h); §1798.140(a).

psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

Limitations on the Definition of Personal Information

The Act excludes the following from the definition of PI:

1. Consumer information that is de-identified or in the aggregate consumer information. This data cannot reasonably be linked to any consumer or household.
2. Information that is publicly available from federal, state, or local government records.

Action Items

- ✓ Determine what types of consumer PI your business collects, shares, and/or sells.
- ✓ Determine whether your business maintains the consumer PI it collects, shares, and/or sells.
- ✓ Determine where, and for how long, your business maintains such consumer PI.
- ✓ Develop a way to identify, track, and control the collection, retention, and deletion of consumer PI.

REQUIRED DISCLOSURES—THE COLLECTION OF PERSONAL INFORMATION[3]

Overview

Once the CCPA comes into effect, businesses will have to make affirmative disclosures to all consumers about the collection and use of PI as defined in the CCPA. Businesses also will have to respond to verifiable consumer requests regarding the company's collection and disclosure of PI.

Automatic Disclosure of General Practices Concerning Personal Information

Under the CCPA, businesses must disclose, at or before collection, the categories of personal information they collect and the purposes for which the personal information will be used. Specifically, businesses will be required to provide the following information—to be updated every 12 months—in their online privacy policies, other relevant company policies, or on their websites:

- A description of consumer rights set forth in the CCPA, including the right to request information concerning the collection and sale of PI, the right to require a business to delete consumer PI, and the right to opt out of any sale by the business of the consumer's PI;
- A description of one or more designated methods for the submission of consumer requests concerning PI;
- A list of the categories of consumer PI that the business has collected in the preceding 12 months;
- A list of the categories of consumer PI that the business has sold in the preceding 12 months—or a statement by the business that it has not sold consumer PI in the preceding 12 months;
- A list of the categories of consumer PI that the business has disclosed for a business purpose in the preceding 12 months—or a statement by the business that it has not sold consumer PI in the preceding 12 months.

Disclosure of Specific Personal Information to Consumers Upon Request

Upon a verifiable consumer request, a business must disclose the following information to the requesting consumer:

- The categories of the consumer's PI that the business collected;
- The categories of sources from which the business collected the consumer's PI;
- The categories of the consumer's PI that the business sold, and the categories of third parties to which it sold the PI;
- The categories of the consumer's PI that the business disclosed for a business purpose;

[3]§1798.100(a); §1798.100(b); §1798.110; §1798.115; §1798.140(t); §1798.140(d).

- The business or commercial purpose for collecting or selling the consumer's PI;
- The categories of third parties with whom the business shared the consumer's PI;
- The specific PI the business has collected concerning the requesting consumer.

A business is not obligated, however, to provide this information to the same consumer more than twice in a 12-month period.

Disclosure Obligations Do Not Create Certain Retention or Linkage Requirements

The CCPA explicitly states that the obligations it imposes on businesses that collect PI do not require a business: (1) To retain any consumer PI for a single one-time transaction if, in the ordinary course of business, such information is not retained; or (2) To re-identify or otherwise link any data that, in the ordinary course of business, is not maintained in a manner that would be considered PI.

Action Items

- ✓ Create a description of consumer rights set forth in the CCPA.
- ✓ Establish a method and process for the submission of consumer requests concerning PI.
- ✓ Draft a written description of this consumer request submission process for publication on the company website.
- ✓ Gather relevant data necessary to identify categories of consumer PI collected, shared, and/or sold—and the categories of third parties with whom consumer PI is shared or sold.
- ✓ Draft a description of the business or commercial purpose for sharing and selling consumer PI.
- ✓ Update online privacy policy and/or company website to comply with CCPA disclosure obligations.
- ✓ Establish internal procedures for fielding, researching, and responding to consumer requests under the CCPA.

KEY CONSUMER RIGHTS

RIGHT TO REQUIRE DELETION OF CONSUMER PERSONAL INFORMATION[4]

Overview

The CCPA establishes the right of consumers to request that a business delete any PI that the business has collected from the consumer—and requires businesses to disclose this right to consumers. If a business receives such a request from a consumer, it must delete the consumer's PI from its records and direct any service providers to delete the consumer's PI from its records.

Exceptions to the Requirement to Delete Consumer PI Upon Request

The CCPA lists several exceptions to a consumer's right to require a business to delete his or her PI. Specifically, a business may deny a verified request if the business can demonstrate that the information is necessary to:

- Complete the transaction for which the PI was collected; provide a good or service requested by the consumer (or one reasonably anticipated within the context of the business' ongoing business relationship with the consumer), or otherwise perform a contract with the consumer;
- Detect security incidents; protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for that activity;
- Debug to identify and repair errors that impair existing intended functionality;
- Exercise free speech, ensure the right of another consumer to exercise his or her right of free speech, or exercise another right provided for by law;
- Comply with the California Electronic Communications Privacy Act;
- Engage scientific, historical, or statistical public-interest research in limited circumstances;
- Enable solely internal uses that are reasonably aligned with the expectation of the consumer based on the consumer's relationship with the business;
- Comply with a legal obligation;
- Otherwise use the consumer's personal information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information.

If the business denies a consumer request under the CCPA, it must inform the customer of the reasons for not taking action and any right to appeal the decision to the business.

[4]§1798.105; §1798.120(a); §1798.135(a)(5); §1798.120(d); §1798.115(d); §1798.135.

Action Items

- ✓ Establish an internal process for dealing with, validating, and logging consumer deletion requests.
- ✓ Identify exceptions to the deletion requirement that are relevant to your business.
- ✓ Establish a communications protocol for responding to customer deletion requests.

RIGHT TO OPT OUT OF THE SALE OF PERSONAL INFORMATION[5]

Overview

The CCPA allows consumers to opt out of a business' sale of its PI and prohibits the business from asking them to change that decision for at least 12 months. In addition, businesses must affirmatively obtain permission from consumers between 13 and 16 years of age, and parental consent from minors younger than age 13, before selling their PI.

Opt Out

The CCPA gives consumers the right, at any time, to direct a business that sells PI about the consumer to third parties not to sell the consumer's PI. This is referred to as the "right to opt out." Businesses that sell consumer PI must provide notice to consumers concerning the fact that consumer PI may be sold and that consumers have a right to opt out of the sale of such information.

The CCPA requires that businesses provide a clear link on their homepage titled, "Do not sell my personal information" that will direct them to a webpage that enables consumers to opt out of the sale of their PI. Moreover, businesses cannot require a consumer to create an account in order to effectuate this opt-out right. Businesses also must provide a description of the opt-out rights, as well as a separate link to the "Do not sell my personal information" webpage, in their online privacy policies, other business policies, or any California-specific description of consumers' privacy rights.

[5]§1798.105; §1798.120(a); §1798.135(a)(5); §1798.120(d); §1798.115(d); §1798.135.

continued on page 11

A business that has received direction from a consumer not to sell the consumer's personal information or, in the case of a minor consumer's personal information has not received consent to sell that personal information, is prohibited from selling the consumer's personal information.

Opt Out: Requests to Sell Information After Opt Out and Third-Party Data Sales

Once a consumer has exercised the consumer's opt-out rights, a business may not request that the consumer authorize the sale of the consumer's PI for at least 12 months.

In addition, a third party may not sell personal information about a consumer that has been sold to that third party by a business, unless the consumer has received explicit notice, and is given an opportunity to opt out.

Action Items

- ✓ Create a "Do not sell my personal information" link/website to satisfy CCPA opt-out rules.
- ✓ Update your online privacy policy and website to satisfy opt-out requirements.
- ✓ Establish a process for tracking consumer opt outs and segregating consumer PI sold to third parties.
- ✓ If your business is a third party recipient of consumer PI, establish a process for providing notice to relevant consumers of any sale of their PI.

RIGHT TO EQUAL SERVICE AND NON-DISCRIMINATION[6]

Overview

The CCPA does not permit a business to discriminate against a consumer because the consumer exercised any of the rights set forth in the statute. For example, businesses may not do the following to consumers who exercise their CCPA rights:

- Deny goods or services to the consumer;
- Charge the consumer different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties;
- Provide different levels or quality of goods or services to the consumer.

[6] §1798.125

A business may, however, charge a consumer a different price or rate, or provide a different level of goods or services to the consumer, if that difference is reasonably related to the value provided to the consumer by the consumer's data.

Businesses also are permitted to offer, on an opt-in basis, "financial incentives" to compensate consumers for the use of their data, but not if the financial incentives are "unjust, unreasonable, coercive, or usurious in nature." For example, a business can offer discounts to consumers who are willing to have their data shared or sold to third parties.

Action Items

- ✓ Calculate the value of consumer data.
- ✓ Consider the development of financial incentive programs that comply with the CCPA.

STATUTORY MECHANISMS FOR CONSUMER ACCESS TO RECORDS

Overview

The CCPA includes many operational details concerning consumer requests under the statute and a business' response. Among other requirements, a business must:

- Make available to consumers two or more designated methods for submitting requests for information required to be disclosed, including, at a minimum, a toll-free telephone number and, if the business maintains an Internet website, a website address;
- Disclose and deliver required information to a consumer free of charge and within 45 days of a verifiable request from a consumer (with the possibility of one 45-day extension);
- Deliver required information by mail or electronically in a portable and readily-usable format;
- Provide the clear and conspicuous homepage link titled, "Do not sell my personal information" for consumers who want to exercise their opt out rights.

The CCPA requires only that businesses deliver information identified in the statute twice a year to consumers upon request.

Action Items

✓ Establish a toll-free telephone number and website for consumer requests pursuant to the CCPA.

✓ Create an internal process for responding to requests that comply with the time limit and format requirements of the CCPA.

ENFORCEMENT, REMEDIES, AND DATA BREACHES[7]

Overview

The California Attorney General may recover statutory damages for violations of the CCPA that are not cured within 30 days of notice to the business (up to $7,500 per intentional violation and up to $2,500 per unintentional violation). The statute also provides for a limited private right of action for a consumer when certain of his or her personal information is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of its duty to implement and maintain reasonable security procedures and practices.

The Private Right of Action

In an effort to remedy violations of the duty to implement and maintain "reasonable security procedures and practices" commensurate with the nature of personal information collected and maintained by companies, the CCPA creates a limited private right of action for a consumer "whose nonencrypted or nonredacted personal information … is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of" this duty. An injured consumer can recover between $100 and $750 per violation, or actual damages (whichever is greater), but first must give the defendant notice of the violation(s), and 30 days to cure the violation(s), before filing a lawsuit. If the business is able to cure the problem within the 30-day window, statutory damages become unavailable.

Importantly, the CCPA incorporates by reference the narrower definition of personal information set forth in Section 1798.81.5(d)(1)(A) for use in determining the viability of a private right of action. This definition states as follows:

> "(1) 'Personal information' means … (A) An individual's first name or first initial and his or her last name, in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted: (i) Social Security number[,] (ii) Driver's license or California identification card number[,] (iii) Account number, credit, or debit card number, in combination with any required security code, access code, or password that would permit access to an individuals' financial account[,] (iv) medical information[,] (v) health insurance information[.]"[8]

The use of this narrower definition of personal information should limit the availability of the CCPA's private right of action.

[7] §1798.155; §1798.150
[8] §1798.81.5

continued on page 15

Current California Data Breach Law Remains Largely Intact

The CCPA leaves the current California statute concerning data breaches and attendant notice obligations, Section 1798.82, untouched. For example, data breach notice requirements will not be governed by the expansive definition of PI contained in the CCPA; rather, the narrower definition set forth in Section 1798.82(h)—which is nearly identical to the definition of personal information in Section 1798.81.5(d)(1)(A) (referenced above and incorporated for purposes of the CCPA's private right of action)—continues to govern these distinct obligations.[9]

Action Items

- ✓ Review your network security to ensure that standards are reasonable—particularly with regard to the collection and maintenance of consumer PI.
- ✓ Upgrade your network security as necessary.
- ✓ Identify appropriate encryption solutions and policies.
- ✓ Identify applicable cyber security legal requirements (e.g., HIPAA, GLBA) and standards (e.g., NIST, CIS, ISO, COBIT, PCI DSS).
- ✓ Conduct privileged assessment of cyber security program and map to applicable legal requirements and standards.
- ✓ Review and revise incident response plan.
- ✓ Address governance issues, including how and when executive leadership manages cyber security and involvement of independent directors.
- ✓ Evaluate risk profile and appetite of company, current levels of applicable insurance coverage, and assess need for additional insurance coverage.

[9]See Glossary for full definition. The most significant difference between Sections 1798.81.5(d)(1)(A) and 1798.82(h) is that Section 1798.82(h) includes a "user name or email address, in combination with a password or security question and answer that would permit access to an online account" in the definition of personal information, while Section 1798.81.5(d)(1)(A) does not.

SIGNIFICANT MISCELLANEOUS PROVISIONS

Overview

There are a number of additional provisions in the CCPA that will have relevance for companies that fall within its scope.

- **Enumerated Exemptions:** The CCPA contains a number of exemptions, which range from those involving conflicting legal obligations (such as when the CCPA restricts a business' ability to: (1) Comply with federal, state, or local law; (2) Comply with civil, criminal, or regulatory inquiries or process; (3) Cooperate with law enforcement; or (4) Exercise or defend legal claims) to those concerning the statute's jurisdictional coverage (such as conduct that takes place wholly outside of California).
- **Ability to Seek an AG Opinion:** The CCPA allows businesses and third parties to seek an opinion of the attorney general for guidance concerning how to comply with the provisions of the law. The statute also gives businesses and third parties 30 days from the date they are notified of noncompliance by the attorney general to cure any related violations.
- **Creation of a Consumer Privacy Fund:** The CCPA creates a Consumer Privacy Fund ("CPF") within the General Fund of the State Treasury. The purpose of the fund is to offset any costs incurred by the AG's office in carrying out its duties under the CCPA, as well as any costs incurred by the state courts in connection with actions brought to enforce the statute. Twenty percent of all civil penalties resulting from the AG's enforcement actions will be directed into the CPF.

SEPTEMBER 2018 AMENDMENTS TO THE CCPA

Overview

In September 2018, the California Legislature passed a series of amendments to the CCPA. While these amendments were styled as technical changes to the law, many are substantive and will have significant implications for businesses.

Amendment Highlights

The following are important amendments made to the CCPA:

- **Elimination of AG Notification and Approval Requirements Concerning Private Right of Actions:** In addition to providing the California Attorney General's Office with more time to draft and adopt regulations to implement the CCPA—and correspondingly delaying the AG's ability to bring enforcement actions until July 1, 2020 (at the latest)—the September 2018 amendments eliminate: (1) The requirement that consumers notify the attorney general once they have brought a private action under the CCPA; and (2) The attorney general's authority to instruct consumers not to proceed with an action.[10]
- **Narrowing of the CCPA's Definition of "Personal Information":** The amendments clarify that PI must identify, relate to, or reasonably link, directly or indirectly, with a particular consumer or household. As a result, data such as IP addresses and geolocation data will not automatically be considered PI for CCPA purposes unless it can be associated with a consumer or household.
- **Expansion of Options Concerning Notice of the Right to Deletion:** The amendments modify the requirement that a business must disclose on its website, or in its privacy policy, a consumer's right to request the deletion of his or her PI; the statute now requires that a business disclose the right to deletion "in a form that is reasonably accessible to consumers."[11]
- **Expansion of Exemptions:** The amendments expand exemptions for data collected, processed, sold, or disclosed, pursuant to the Gramm-Leach-Bliley Act and Driver's Privacy Protection Act, by removing language that had limited these exemptions to situations where the laws conflicted with the CCPA. As a result, data covered by these laws is now entirely exempt from the CCPA's ambit. In addition, the amendments add an exemption for data collected, processed, sold, or disclosed pursuant to the California Information Privacy Act, and expand or add exemptions concerning protected health information, clinical trial data, and the applicability of the law to health care providers under certain circumstances.
- **Updates Relating to Constitutional Matters**: The amendments include a provision designed to exempt "noncommercial activities of a person or entity" from the CCPA's coverage to protect activities of the press in response to First Amendment concerns. They also add a preemption clause concerning the United States Constitution.

[10] §1798.150(b)
[11] §1798.105(b)

GDPR COMPARISON

Overview

The CCPA and the GDPR are significantly different. The GDPR is a far-reaching regulation that encompasses a broad array of compliance topics—including personal data processing principles, the requirement that any personal data processing must have a legal basis, various rights of any data subjects (not just consumers) in the context of data processing, accountability, and governance mechanisms for data processing, requirements for data security and an obligation of data breach notification—and conditions for the international transfer of personal data. In contrast, the CCPA focuses mainly on effectuating data privacy rights by giving consumers knowledge concerning, and more control over, the collection and use of their PI.

Comparison Highlights

There are a number of significant differences between the CCPA and GDPR, including the following:

- Both the CCPA and the GDPR contain broad definitions of "personal information" or "personal data." Both the GDPR and the CCPA extend to data that can be linked to an individual (CCPA) or that can be used to identify an individual (GDPR). Unlike the GDPR, however, the CCPA covers information about a particular individual and a household and excludes data that is publicly available. There is no definition for sensitive data—which trigger heightened GDPR obligations—under the CCPA.
- The CCPA is narrower than the GDPR in a number of aspects. It applies only to entities that: (i) Are what would be referred to under the GDPR as "controllers"; (ii) Do business in California (unless every aspect of the entity's commercial conduct concerning the collection and sale of personal information takes place outside of California); and (iii) Exceed one of the CCPA's financial or personal information activity thresholds. By contrast, the GDPR applies to processing taking place inside and outside the European Union and applies to companies that do not have any establishments in the European Union if they process personal data about subjects who are in the European Union (i.e., when offering goods and services to such data subjects or monitoring their behavior in the European Union) and do not contain financial thresholds.
- Unlike the GDPR, the CCPA does not contain overarching data processing principles and instead imposes specific, limited restrictions on what a business can do with personal data.

continued on page 19

- The presumption under the CCPA is that the processing of personal information is allowed. Under the GDPR, any processing of personal data is unlawful unless it can be justified under one of six legal grounds.
- Under the CCPA, businesses can "sell" personal information and consumers have a right to opt out of the selling. In contrast, the GDPR includes broader rights for data subjects to restrict and object to the processing of their personal data more generally.
- The GDPR contains rights of access, rectification, correction, erasure, and restriction, as well as a right to data portability and the right to object to data processing. The CCPA provides for five rights of California residents, but only the right to access is very similar.
- Unlike the GDPR, the CCPA does not specifically restrict data transfers to other countries.

ACTION ITEMS LIST

- Determine whether your company meets the $25 million annual revenue threshold.
- Assess your company's practices concerning the collection and use of personal information.
- Ascertain how the collection and use of personal information affects your revenues.
- Determine what types of consumer PI your business collects, shares, and/or sells.
- Determine whether your business maintains the consumer PI it collects, shares, and/or sells.
- Determine where, and for how long, your business maintains such consumer PI.
- Develop a way to identify, track, and control the collection, retention, and deletion of consumer PI.
- Create a description of consumer rights set forth in the CCPA.
- Establish a method and process for the submission of consumer requests concerning PI.
- Draft a written description of this consumer request submission process for publication on the company website.
- Gather relevant data necessary to identify categories of consumer PI collected, shared, and/or sold—and the categories of third parties with whom consumer PI is shared or sold.
- Draft a description of the business or commercial purpose for sharing and selling consumer PI.
- Update online privacy policy and/or company website to comply with CCPA disclosure obligations.
- Establish internal procedure for fielding, researching, and responding to consumer requests under the CCPA.
- Establish an internal process for dealing with, validating, and logging consumer deletion requests.
- Identify exceptions to the deletion requirement that are relevant to your business.
- Establish a communications protocol for responding to customer deletion requests.
- Create a "Do not sell my personal information" link/website to satisfy CCPA opt-out rules.
- Update your online privacy policy and website to satisfy opt-out requirements.
- Establish a process for tracking consumer opt outs and segregating consumer PI sold to third parties.

continued on page 21

ACTION ITEMS LIST

- Establish a process for providing notice to relevant consumers of any sale of their PI if your business is a third party recipient of consumer PI.
- Calculate the value of consumer data.
- Consider the development of financial incentive programs that comply with the CCPA.
- Establish a toll-free telephone number and website for consumer requests pursuant to the CCPA.
- Create an internal process for responding to requests that comply with the time limit and format requirements of the CCPA.
- Review your network security to ensure that standards are reasonable, particularly with regard to the collection and maintenance of consumer PI.
- Upgrade your network security as necessary.
- Identify appropriate encryption solutions and policies.
- Identify applicable cyber security legal requirements (e.g., HIPAA, GLBA) and standards (e.g., NIST, CIS, ISO, COBIT, PCI DSS).
- Conduct privileged assessment of cyber security program and map to applicable legal requirements and standards.
- Review and revise incident response plan.
- Address governance issues, including how and when executive leadership manages cyber security and involvement of independent directors.
- Evaluate risk profile and appetite of company, current levels of applicable insurance coverage, and assess need for additional insurance coverage.

GLOSSARY

Aggregate consumer information	Information that relates to a group or category of consumers, from which individual consumer identities have been removed, that is not linked or reasonably linkable to any consumer or household, including via a device. This does not mean one or more individual consumer records that have been de-identified. (§1798.140(a))
Business	(1) A sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that collects consumers' personal information, or on the behalf of which such information is collected; that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information; that does business in the State of California, and that satisfies one or more of the following thresholds: (A) Has annual gross revenues in excess of $25 million dollars ($25,000,000), as adjusted pursuant to paragraph (5) of subdivision (a) of Section 1798.185. (B) Alone or in combination, annually buys, receives for the business' commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices. (C) Derives 50 percent or more of its annual revenues from selling consumers' personal information. (§1798.140(c))
Consumer	A natural person who is a California resident, however identified, including by any unique identifier. (§1798.140(g); Cal. Rev. & Tax. Code §17014)

De-identified	Information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, provided that a business that uses de-identified information takes certain actions. (§1798.140(h))
Probabilistic identifier	Identification of a consumer or a device to a degree of certainty of more probable than not based on any categories of personal information included in, or similar to, the categories enumerated in the definition of personal information. (§1798.140(p))
Processing	Any operation or set of operations that are performed on personal data or on sets of personal data, whether or not by automated means. (§1798.140(q))
Pseudonymize or Pseudonymization	The processing of personal information in a manner that renders the personal information no longer attributable to a specific consumer without the use of additional information, provided that the additional information is kept separately and is subject to technical and organizational measures, to ensure that the personal information is not attributed to an identified or identifiable consumer. (§1798.140(r))

Personal information under the CCPA	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, the following (if it identifies, relates to, describes, is capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household): (A) Identifiers, such as a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, Social Security number, driver's license number, passport number, or other similar identifiers. (B) Any §1798.80(e) categories of personal information. (C) Characteristics of protected classifications under California or federal law. (D) Commercial information, including records of personal property; products or services purchased, obtained, or considered; or other purchasing or consuming histories or tendencies. (E) Biometric information. (F) Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an Internet website, application, or advertisement. (G) Geolocation data. (H) Audio, electronic, visual, thermal, olfactory, or similar information. (I) Professional or employment-related information. (J) Education information that is not publicly available or personally identifiable, as defined in the Family Educational Rights and Privacy Act (20 U.S.C. §1232g, 34 C.F.R. Part 99). (K) Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes. (§1798.140(o))

Personal information under the California Consumer Records Act's security procedures and practices provision (incorporated by reference in the CCPA's private cause of action provision)	(A) An individual's first name or first initial and his or her last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted: (i) Social Security number. (ii) Driver's license number or California identification card number. (iii) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account. (iv) Medical information. (v) Health insurance information. (Cal. Civ. Code §1798.81.5(d)(1)(A))
Personal information under the California Consumer Records Act's data breach notification provision (not referenced in the CCPA)	1) An individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (A) Social Security number. (B) Driver's license number or California identification card number. (C) Account number or credit or debit card number, in combination with any required security code, access code, or password, that would permit access to an individual's financial account. (D) Medical information. (E) Health insurance information. (F) Information or data collected through the use or operation of an automated license plate recognition system, as defined in Section 1798.90.5. (2) A user name or email address, in combination with a password or security question and answer, that would permit access to an online account. (Cal. Civ. Code §1798.82(h))

CONTACT INFORMATION

Americas

Daniel J. McLoon

Los Angeles
+1.213.243.2580
djmcloon@jonesday.com

Edward S. Chang

Irvine
+1.949.553.7561
echang@jonesday.com

Aaron D. Charfoos

Chicago
+1.312.269.4242
acharfoos@jonesday.com

Ryan M. DiSantis

Boston
+1.617.449.6911
rdisantis@jonesday.com

Christopher Hurld

Boston
+1.617.449.6907
churld@jonesday.com

Samir C. Jain

Washington
+1.202.879.3848
sjain@jonesday.com

Richard J. Johnson

Dallas
+1.214.969.3788
jjohnson@jonesday.com

J. Todd Kennard

Columbus
+1.614.281.3989
jtkennard@jonesday.com

James T. Kitchen

Pittsburgh
+1.412.394.7272
jkitchen@jonesday.com

Guillermo E. Larrea

Mexico City
+52.55.3000.4064
glarrea@jonesday.com

Richard M. Martinez

Minneapolis
+1.612.217.8853
rmartinez@jonesday.com

Todd S. McClelland

Atlanta
+1.404.581.8326
tmcclelland@jonesday.com

Mauricio F. Paez

New York
+1.212.326.7889
mfpaez@jonesday.com

Jeff Rabkin

San Francisco / Silicon Valley
+1.415.875.5850 / +1.650.739.3954
jrabkin@jonesday.com

Lisa M. Ropple

Boston
+1.617.449.6955
lropple@jonesday.com

John A. Vogt

Irvine
+1.949.553.7516
javogt@jonesday.com

continued on page 27

Europe, the Middle East, and Africa

Olivier Haas

Paris
+33.1.56.59.38.84
ohaas@jonesday.com

Dr. Undine von Diemar

Munich
+49.89.20.60.42.200
uvondiemar@jonesday.com

Dr. Jörg Hladjk

Brussels
+32.2.645.15.30
jhladjk@jonesday.com

Jonathon Little

London
+44.20.7039.5224
jrlittle@jonesday.com

Asia-Pacific

Chiang Ling Li

Hong Kong
+852.3189.7338
chianglingli@jonesday.com

Michiru Takahashi

Tokyo
+81.3.6800.1821
mtakahashi@jonesday.com

Adam Salter

Perth
+61.8.6214.5720
asalter@jonesday.com