DATA PRIVACY AND CYBERSECURITY

CALIFORNIA'S DATA PRIVACY LAW: WHAT IT IS AND HOW TO COMPLY (A STEP-BY-STEP GUIDE)

by Sara H. Jodka

Just as U.S. companies were settling into the idea of the EU's General Protection Act (GDPR), California just passed the California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100 *et seq*. (CCPA), which will require U.S. companies to implement a number of similar privacy initiatives, which will afford California residents unparalleled (in the United States) data privacy rights. The law takes effect on January 1, 2020, and the following summarizes the law, including who it applies to and how, and offers a step-by-step guide to compliance.

What Businesses Must Comply with the CCPA?

Subject to a number of exceptions, discussed below, the CCPA covers every "business" that collects and sells consumer "personal information" or discloses personal data for a business purpose.

Going through the relevant definitions, a "business" is a for-profit legal entity doing business in California that collects personal information regarding California residents. Following well-established jurisprudence, the scope of "doing business" in California applies to companies that sell goods or services to California residents *even if the business is not physically located in California*. Its application beyond U.S. borders could significantly expand the impact of the legislation.

Not all business qualify. To fall within the scope of the CCPA, the business must also meet one of the additional *three* criteria:

- Have $25 million or more in annual revenue; or
- Possess the personal data of more than 50,000 "consumers, households, or devices" or
- Earn more than half of its annual revenue selling consumers' personal data.

As for what constitutes "personal information", that term is defined broadly as "information that identifies, relates to, describes, is capable of being associated with, or could reasonable be linked, directly or indirectly, with a particular California resident or household." The definition of "personal information" includes:

- Personal identifiers, such as a real name, alias, postal address, unique personal identifier, IP address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers;
- Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies;
- Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a California resident's interaction with an internet web site, application, or advertisement;
- Geolocation data;
- Biometric information;
- Audio, electronic, visual, thermal, olfactory, or similar information;
- Professional or employment-related information; and
- Education information.

A "consumer" is a natural person (so not a legal entity such as a corporate) who is a California resident, which includes every individual who is in the state for other than a temporary or transitory purpose, or every individual who is domiciled in the state who is outside the state for a temporary or transitory purpose. The definition is quite broad, which means it appears to cover California residents *while they are traveling in other states.*

Exclusions

The CCPA's obligations do not restrict a business' ability to collect or sell a consumer's personal information if every aspect of that commercial conduct takes place completely outside of California. In other words, if the business collected the consumer's personal information while the consumer was outside California, no part of the sale of the consumer's personal information occurred in California, and no personal information collected while the consumer was in California is sold.

The CCPA also does not apply to information that is subject to other federal regulation, including, the Health Insurance Portability and Accountability Act (HIPAA); the Gramm-Leach Bliley Act (GLBA); the Fair Credit Reporting Act (FCRA); or the Drivers' Privacy Protection Act (DPPA), The CCPA, however, will apply to entities covered by these laws to the extent they collect and process other personal information about consumers.

What Rights the CCPA Afforded Consumers?

The CCPA will provide consumers with new rights, including a right to transparency about data collection, a right to be forgotten, and a right to opt out of having their data sold (opt in for minors).

While the list of rights may seem largely identical to the list of rights guaranteed to EU data subject under the GDPR, there are a number of significant differences, one being that the GDPR is structured as an opt-out mechanism as opposed to the GDPR's confusing opt-in mechanism.

The opt-out structure of the CCPA grants consumers the following rights and does the following:

The right to know whether their personal information is being collected about them
• Requires businesses to make disclosures to consumers about any personal information collected and the purposes for which the personal information is used.
The right to request the specific categories of information a business collects upon verifiable request
• Grants consumers a right to request that a business disclose the categories and specific pieces of personal information that the business collects about them, the categories of sources from which that information is collected, the business purposes for collecting or selling the information, and the categories of third parties with which the information is shared.
The right to know what personal information is being collected about them
• Requires businesses to make disclosures to consumers about any personal information collected and the purposes for which the personal information is used. • Grants consumers a right to request that a business disclose the categories and specific pieces of personal information that the business collects about them, the categories of sources from which that information is collected, the business purposes for collecting or selling the information, and the categories of third parties with which the information is shared.
The right to say "no" to the sale of personal information
• Authorizes consumers to opt out of the sale of personal information by a business and prohibits the business from discriminating against the consumer for exercising this right, including by charging the consumer who opts out a different price or providing the consumer a different quality of goods or services, except if the difference is reasonably related to value provided by the consumer's data. • Prohibits a business from selling the personal information of a consumer under 16 years of age, unless affirmatively authorized. • ***The definition of the word "sell" for purposes of the CCPA is broad and includes, "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 third party for monetary or valuable consideration."*
The right to delete their personal information
• Grants consumers the right to request deletion of personal information and would require the business to delete personal information upon receipt of a verified request.
The right to equal service and price, even if they exercise their privacy rights
• Authorizes businesses to offer financial incentives for collection of personal information

Step-By-Step Compliance

For those companies that had to comply with the GDPR, the CCPA should be a piece of cake. For those that did not, well, those companies can learn a lot from those still recovering (or still suffering) from GDPR heartburn. Below are some key steps to CCPA compliance:

Step 1: Update Privacy Notices and Policies

With *all* the "We've updated our Privacy Policy" (GDPR-compliance) emails received in May 2018, it is probably reasonable to expect another wave, this time CCPA compliant, in December 2019.

The California Online Privacy Protection Act of 2003 already requires companies who process the personal information of California consumers through commercial websites to post a privacy notice, and companies that had to be GPDR compliance added additional information to those privacy notices in early 2018.

The CCPA will require that "at or before the point of collection" covered companies provide notice to consumers informing them of the categories of personal information the company collects and what purpose the information is used by the company.

The notice must also explicitly set forth the categories of personal information that are collected, disclosed, or sold (*see* broad definition discussed above), and consumers have a new right to opt-out of having their information sold.

Companies will also need to update their privacy policies to include a description of the other new consumer rights afforded by the CCPA (*see* chart above).

As many companies had to determine when becoming GDPR compliant, prior to making the legally-required policy updates, companies will need to determine if they will maintain one privacy notice for California residents and one for other consumers, or have one universal policy.

Step 2: Update Data Inventories, Business Processes, and Data Strategies

Companies will also have to maintain a data inventory, which is essentially a database to track their data processing activities, including the business processes, third parties, products, devices, and applications that process consumer personal data.

Companies that had to become GDPR compliant will have to add a few columns to their data inventories including, a column:

1. identifying if the data use includes the "sale" of information;

2. identifying what categories of personal information are transferred to third parties;

3. identifying if any categories of personal information are covered by HIPAA, the FCRA, or another law that would exempt the data from the CCPA's scope; and

4. identifying if the data was collected more than 12 months ago and, thus, potentially exempt.

The database will also have to be kept up to date and be able to track all consumer right requests, such as tracking a verified request for information.

Step 3: Implement Protocols to Ensure Consumer Rights

As set forth more summarily above, the CCPA guarantees a number of consumer rights that businesses will need to take steps to ensure.

Right to Notice	While it is not exactly a granted right, at or before a business collects personal information from a consumer, the consumer must be properly notified which categories of information are being collected and the purposes for which the information is being used.
Right of Access / Right to Request	Upon verifiable request, the business must take steps to disclose and deliver, free of charge to the consumer, the personal information, which may be delivered by mail or electronically. If provided electronically, it must be provided in a portable and, to the extent technically feasible, in a readily usable format that allows the consumer to transmit the personal information to another entity without issue. A business may provide personal information to a consumer at any time, but does not have to provide it to a consumer more than twice in a 12-month period. (*Note:* This does not require a business to retain personal information that is collected for a single one-time transaction if the information is not sold or retained by the business or to re-identify or otherwise link information that is not maintained in a manner that would be considered personal information.)
Right to Know	The consumer has the right to request that a business that collects personal information disclose the following: (1) the categories of personal information collected; (2) the sources from which the information was collected; (3) the business or commercial purpose for collecting or selling the information; (4) categories of third parties with whom the business shares the information; (5) the specific pieces of personal information the business collected about the consumer. (*Note:* this does not require a business to retain personal information that is collected for a single one-time transaction if the information is not sold or retained by the business or to re-identify or otherwise link information that is not maintained in a manner that would be considered personal information.)
Right to Delete	The consumer has the right to request, upon verifiable request, that a business delete any personal information about the consumer the business has collected. Upon receipt of such request, the business must delete the information and direct any service providers to delete the information from its records as well unless the business or service provider needs the information to: (1) compute the transaction for which the personal information was collected, provide a good or service requested by the consumer, or reasonably anticipated within the context of a business's ongoing business relationship with the consumer, or otherwise perform a contract between the business and the consumer; (2) detect security incidents; protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for that activity; (3) debug to identify and repair errors existing intended functionality; (4) exercise free speech, ensure the right of another consumer to exercise his/her right of free speech, or exercise another right provided for by law; (5) comply with the California Electronic Communications Privacy Act; (6) engage in public or peer-received scientific, historical, or statistical research in the public interest; (7) to enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business; (8) comply with a legal obligation; (9) 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.

Right to Opt Out	The consumer has the right to opt out of the sale of personal information by a business. Businesses must make available, in a form reasonably accessible to consumers, a clear and conspicuous link to the homepage, titled "Do Not Sell My Personal Information" that enable a consumer to opt-out of the sale of the consumer's personal information. The business must wait at least 12 months before requesting to sell the personal information of any consumer who has opted out. If the consumer's information is sold, the consumer has additional rights and can request a business that sells or discloses the information for a business purpose, disclose to the consumer: (1) the categories of personal information the business collected about the consumer; (2) the categories of information the business sold about the consumer and the categories of third parties to whom the information was sold, by category or categories of information for each third part to whom the information was sold; and (3) the categories of information the business disclosed about the consumer for a business purpose. With this, a third party is prohibited from selling information about a consumer that has been sold to the third party by a business unless the consumer has received explicit notice and is provided the opportunity to opt out.
Right to Notification of Financial Incentive	A business may charge a consumer a different price or rate, or from providing a different level or quality 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 may offer financial incentives, including payments to consumers as compensation, for the collection of information, the sale of personal information, or the deletion of information. A business may also offer a different price, rate, level, or quality of goods or services to the consumer if that price or difference is directly related to the value provided to the consumer by the consumer's data. If a business offers financial incentives it must notify customers of them. A business may enter a consumer into a financial incentive program only if the consumer gives the business prior opt-in consent that clearly describes the material terms of the financial incentive program, and which may be revoked by the consumer at any time.
Right Not to Be Discriminated Against	Businesses are prohibited from discriminating against a consumer for exercising any of the consumer's rights, including by: (A) denying goods or services to the consumer; (B) charging different prices or rates for goods or services, including the use of discounts or other benefits or imposing penalties; (C) providing a different level or quality of goods or services to the consumer; or (D) suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services. The prohibition on discrimination, however, does not prohibit a business from charging a consumer a different price or rate, or from providing a different level or quality 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 may offer financial incentives, including payments to consumers as compensation, for the collection of information, the sale of personal information, or the deletion of information. A business may also offer a different price, rate, level, or quality of goods or services to the consumer if that price or difference is directly related to the value provided to the consumer by the consumer's data. If a business offers financial incentives it must notify customers of them. A business may enter a consumer into a financial incentive program only if the consumer gives the business prior opt-in consent that clearly describes the material terms of the financial incentive program, and which may be revoked by the consumer at any time.

To ensure consumers can exercise their rights to: (1) request information about what information the business collects and what it does with the information; (2) request that the business delete any personal information collected; and (3) not be discriminated against, **the business must make available to consumers at least two designated methods for submitting requests for information, including, at a minimum, a toll-free telephone number and, if the business has a Website, a Website address.**

The business also must ensure it has protocols in place to respond to such requests free and within 45 days of receiving a verifiable request.

This information must be disclosed in the business's online privacy policy or in any California-specific description of consumers' privacy rights, and the information must be updated at least once every 12 months.

This is what a roll-out may look like in application:

1. Ensure data inventory is up-to-date and contains all required information, which will include defining the businesses record systems and designated records sets to be used as the authoritative data sets for all CCPA purposes;

2. Update all relevant policies, including any California-specific descriptions concerning consumers' privacy rights;

3. Update policies to provide for data subject requests, including a toll-free number or Website address;

4. Determine a process for documenting consumer requests, which must include a protocol for authenticating requests, timely responding to requests, effected a "stop-the-sale-of-information" order; and denying improper or untimely requests;

5. Training employees who handle consumer requests on the businesses' relevant privacy policies and procedures to ensure timely processing, responding, monitoring, and updating of the data inventory;

6. Ensuring data inventory processes are kept up to date as new consumer information is collected and deleted;

7. Ensuring consumers who opted out of the sale of their information are not asked to re-consent before 12 months of their opting out has passed;

8. Update all relevant privacy policies once every 12 months.

Step 4: Make Security Updates

The CCPA requires covered businesses protect personal data with "reasonable" security. In practice, this standard has led companies to take a risk-based approach toward addressing threats to the confidentiality, integrity, and availability of personal data. They assess the threats to data, rank the risks of the detected vulnerabilities, and address the high-risk gaps first. For not a few corporations, the cost of addressing high-risk gaps is staggering, and some accept the risk of not mitigating some medium-risk gaps.

Step 5: Update Third-Party Processor Agreements

To comply with the CCPA, businesses that have other companies process their data will need to update their third party contracts including inserting standard-contractual clause language; requiring vendor data inventories; using due diligence questionnaires; providing records of processing; requiring the syncing of consumer response processes; requiring onsite assessment and auditing; and requiring mapping of the specific data elements shared with each third party, including designating those transfer that qualify as "selling".

For those third-party that paid for information, they will need to additionally design processes to accommodate consumer requests to opt out of selling and provide for the deletion of that data.

Step 6: Training

The CCPA requires that employees handling consumer inquiries be informed of *all* of its requirements. Due to the penalties involved (*see* below) this training should be the minimum and additional employee training is recommended.

Penalties

The CCPA will generally be enforced by the Attorney General, but it does provide for a private right of action in instances where there is certain unauthorized access and exfiltration, theft, or disclosure of non-encrypted or non-redacted personal information.

If "non-encrypted or non-redacted" consumer information is compromised because of a failure of reasonable security, a consumer may bring a legal action for statutory damages ranging from $100 to $750 per violation or actual damages, whichever is greater.

All other penalties are driven by the Attorney General. The AG may target the reasonability of a company's security measures, but the AG is also responsible for pursuing statutory penalties and those penalties can go up to $7,500 per violation.

This client alert is published by Dickinson Wright PLLC to inform our clients and friends of important developments in the field of Data Privacy and Cybersecurity law. The content is informational only and does not constitute legal or professional advice. We encourage you to consult a Dickinson Wright attorney if you have specific questions or concerns relating to any of the topics covered in here.

FOR MORE INFORMATION CONTACT:

Sara H. Jodka is Of Counsel in Dickinson Wright's Columbus office. She can be reached at 614.744.2943 or sjodka@dickinsonwright.com.