Reinhart

The California Consumer Privacy Act: What You Need to Know About the Nation's Toughest Privacy Law

Touted as the toughest privacy law in the United States, the California Consumer Privacy Act (CCPA) takes effect January 1, 2020, with enforcement slated to begin July 1, 2020. The CCPA requires certain businesses to implement privacy initiatives designed to protect California residents (referred to in the CCPA as "consumers").

Businesses that Must Comply

Any business, regardless of where it is headquartered, that collects and controls consumers' personal information and meets the following criteria must comply with the CCPA:

- For profit business;
- Does business in California; AND
- Meets one or more of the following:
    1. Has annual gross revenues in excess of $25 million;
    2. Annually receives, buys, sells, or shares, directly or indirectly, the personal information of 50,000 or more California consumers, households, or devices; OR
    3. Derives 50% or more of its annual revenue from selling California consumers' personal information.

When is a business "doing business in California"?

While the CCPA does not specifically define when a business is "doing business in California," the phrase is used in California tax law, which states the following factors should be considered:

1. Headquarters is in California
2. Employees are in California
3. The business is required to qualify in California as a foreign entity

POSTED:

Oct 7, 2019

RELATED PRACTICES:

Corporate Law
https://www.reinhartlaw.com/practices/corporate-law

Health Care
https://www.reinhartlaw.com/practices/health-care

Banking and Finance
https://www.reinhartlaw.com/practices/banking-and-finance

RELATED SERVICES:

Data Privacy and Cybersecurity
https://www.reinhartlaw.com/services/data-privacy-and-cybersecurity

Emerging Businesses and Early-Stage Investing
https://www.reinhartlaw.com/services/emerging-businesses

Employment Counseling, Advice and Compliance
https://www.reinhartlaw.com/services/employment-counseling-advice-and-compliance

Financial Institutions
https://www.reinhartlaw.com/services/financial-institutions

Health Care Technology and Innovation
https://www.reinhartlaw.com/services/health-care-technology-and-innovation

Arizona/California/Florid

4. Repeated sales into the state

It's important to note that a business may be "doing business in California" even if it's not physically present in the state.

What is personal information?

The CCPA defines "personal information" more broadly than what is provided under most other state laws: "Personal information" is "[i]nformation 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.[1] This includes, but is not limited to, information such as:

- Identifiers (*e.g.*, legal name, postal address, e mail address, social security number, driver's license number, and passport number)
- Commercial information (*e.g.*, records of personal property, products or services purchased, and other purchase histories)
- Biometric information
- Internet activity (*e.g.*, browsing history, search history, and information related to a consumer's interaction with a website)
- Geolocation data
- Education information
- Professional and employment information
- Audio, electronic, visual, thermal, olfactory or similar information

Put simply, if the information is about a person, or can "reasonably be associated with" a person, it is likely "personal information" under the CCPA.

Consumer Rights under the CCPA

The CCPA requires that, "at or before the point of collection," a business provide notice to consumers of the categories of personal information collected, the purpose for which the information is collected, and the categories of third parties with whom the business will share such personal information. The business must also notify consumers of the categories of personal information that are disclosed or sold. These consumer rights must be outlined in a privacy policy, and updated

a/Illinois/South Dakota Law Consultations
https://www.reinhartlaw.com/services/arizonacaliforniafloridaillinoissouth-dakota-law-consultations

RELATED PEOPLE:

Martin J. McLaughlin
https://www.reinhartlaw.com/people/martin-mclaughlin

at least every 12 months.

Consumers have the right to request that their personal information be deleted, and a business must notify consumers of this right in a "reasonably accessible" manner. The business must communicate such requests to its service providers and data processors and ensure they also comply with such requests. CCPA section 130 provides a business must "[d]isclose and deliver the required information to a consumer … within 45 days of receiving a verifiable" request from the consumer.

Consumers are permitted to obtain a digital copy of their personal information, up to twice per 12 month period, in a format that allows him or her to transfer the information to another business.

Under the CCPA, consumers can prohibit the sale of their individual personal information. To accommodate such a request, a business should implement an opt out request as well as an opt in authorization to provide for the possibility of a consumer later changing his or her mind. A request to opt out must be made in a verifiable manner, such as from a consumer's password protected account. A business must not ask a consumer to opt back in to the sale of his or her personal information for a minimum of 12 months after the consumer has opted out.

Under the CCPA, consumers must also be afforded the "right to equal service and price." This means a business cannot penalize a consumer for exercising his or her rights under the CCPA by denying the provision of goods or services, charging a different price, or imposing penalties.

Exceptions to Consumer Rights under the CCPA

The CCPA does not apply to "personal health information," as defined by the Health Insurance Portability and Accountability Act of 1996 (HIPAA), personal information processed under the Gramm Leach Bliley Act, or personal information collected or processed within the context of consumer reporting pursuant to the Fair Credit Reporting Act.

The California Assembly has also approved a number of CCPA amendments that create exceptions to the rights and obligations promulgated thereunder:

- Personal information collected from job applicants, employees, contractors, or agents is not covered under the CCPA.
- A business may sell consumer personal information collected as part of a

loyalty, reward, club card, or discount program, as long as the consumer has provided express consent and the third party uses the personal information only to determine eligibility for a financial incentive.

- Once a consumer has requested that his or her personal information be deleted, a business may retain such personal information, as long as it's retained so as to provide it to a government agency "for purposes of, or in furtherance of, a government program."
- The CCPA does not apply to vehicle or vehicle ownership information retained or shared "for the purpose of effectuating, or in anticipation of effectuating, a vehicle repair covered by a vehicle warranty or a recall."
- Insurance institutions, agents, and insurance support organizations are exempt from CCPA requirements regarding personal information retained or shared for the purpose of completing an insurance transaction.
- Retention of personal information is permitted for certain businesses (e.*g.*, to provide a good or service requested by the consumer) and for legal purposes (*e.g.*, to satisfy an official request from the government, etc.).

Complying with the CCPA

Businesses should revise their privacy policies so as to clearly define the categories of personal information collected, the uses of such information, and consumer rights under the CCPA.

Generally, businesses must have two methods by which a consumer can submit a CCPA related request, one of which must be a toll free telephone number. However, if a business operates solely online and has a direct relationship with the consumer, the business is only required to provide an e mail address and a website via which the consumer can request a copy of or the deletion of his or her personal information.

Businesses should also implement data strategies that track the types of personal information collected and/or sold, the uses of such information, and the third party products or parties used to collect or process the personal information. These data strategies should include a system to track when consumer requests are received, when notice has been provided to the consumer that the request has been received, and when the request has been fulfilled.

Under the CCPA, businesses must maintain "reasonable security" procedures to protect personal information from "unauthorized access, exfiltration, theft or disclosure." The CCPA does not define what constitutes "reasonable security"; however, complying with a recognized information security framework, such as the Center for Internet Security (CIS), the National Institute of Standards and Technology Cybersecurity Framework, or the International Organization of Standardization, will demonstrate "reasonable security" procedures.[2]

Finally, agreements with third party processors and service providers should be revised so as to comply with the CCPA.

Penalties for Non-Compliance

California's Office of the Attorney General is empowered to bring an action against a business that has failed to meet compliance requirements of the CCPA. The CCPA provides for fines of up to $2,500 per violation, or $7,500 per intentional violation. If personal information that has not been redacted or encrypted is subject to unauthorized access, the CCPA provides for a private right of action. Such an action cannot be brought, however, if the business cures the violation within 30 days and notifies the aggrieved consumer in writing that the issue has been addressed and guaranties no further violations will occur.

[1] Consumers are those individuals who are in the state for a purpose that is not temporary or transitory and includes every individual who is domiciled in California even when outside of the state for a temporary or transitory purpose.

[2] In a 2016 Data Breach Report, the California Attorney General endorsed the CIS Controls as reasonable security practices, which include, among other recommendations, the controlled use of administrative privileges and the implementation of malware defenses.