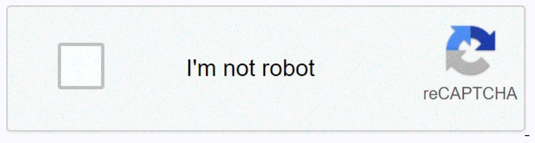

Continue

California consumer privacy act compliance guide

The recently passed California Consumer Privacy Act 2018 (the CCPA) represents a significant new compliance burden for most businesses that collect personal information about California residents. A slice of GDPR in California? The passage of the CCPA comes at a time when many US companies with international activities are still dealing with the significant compliance burden associated with the General Data Protection Regulation (GDPR) and, despite some similarities, the CCPA imposes additional burdens on businesses covered by both systems. We will carefully analyse the new obligations imposed on the undertakings concerned by the CCPA. Read the full article here. CCPA and GDPR: For many multinationals, understanding the similarities and differences between CCPA and GDPR will be a key element in effectively managing compliance between both systems. See a comparison of each key provision here. CCPA 100-day compliance checklist: This isn't just a privacy policy time running out to comply with California's Consumer Privacy Act (CCPA). Companies need to take a number of steps to ensure that they comply with the 2020 financial year. Read the full article here. UK Business Exposure to California Consumer Privacy Act (2018) (CCPA) Ccpa 2020. Read the full article here. Do Turkish companies have to comply with the California Consumer Privacy Act (CCPA)? Your business complies with General Data Protection Regulation 6698 and/or the Turkish Personal Data Protection Act and its Secondary Law (PDPL); but does it comply with the California Consumer Privacy Act (CCPA), which will be applicable until 31 December 2020? If your company needs to comply with ccpa, some important differences should be taken into account in managing data protection compliance. Read the full article here. The California Consumer Privacy Act regulations ended up here, but wait there's more... White & Case LLP's F. Paul Pittman and Kyle Levenberg discuss newly approved California Consumer Protection Act (CCPA) regulations that establish specific content and administrative compliance obligations for businesses covered by the CCPA. See also White & Case Technology Newsflash This publication is for your convenience and does not constitute legal advice. This publication is copyrighted. © 2019 White & Case LLP May 2020 Update: California votes in November on a major update to california's consumer privacy law. This law is called the California Data Protection Act (CPRA). This includes the new executive agency, new personal data terminology, clear how to comply, and so on. You can read about these proposed changes here. We'll do it. if we know the final rules. California's new privacy law is officially the notice to protect consumers' personal information under California Consumer Protection Act (CCPA) a new consumer privacy law that has been through a voting initiative and took effect on January 1, 2020. This means that you only had a few months to not only understand, but also make sure that you, the company and your employees are all doing what you need to do to protect consumers' personal information and comply with the regulations. Remember, while this is a California assignment, it doesn't just apply to California residents. Almost every company that does business with a California company, california-based customers, or collects personal information from a California resident for any purpose (customer or non-customer), must comply. It is important to understand that all divisions of the company are responsible and have the potential to put the company at risk. Like the GDPR, the risk of non-compliance can be a heavy fine and loss of customer loyalty. Understanding the California Consumer Privacy Act (CCPA) If you don't have a legal background, the CCPA parlance may seem complicated and somewhat confusing. That's why we want to tear it down for you. This is a critical new regulation with serious consequences. No matter your background or your current role, you will not be able to circumvent the ignorance card. It's up to us to do this right. What is the California Consumer Privacy Act (CCPA)? The California Consumer Privacy Act is often referred to as CCPA. It's a bill passed by california's state legislature in 2018, but didn't take effect until January 2020. Like the European Union General Data Protection Regulation (GDPR), ccpa forces the hands of many (but not all) organisations to protect consumers' data protection rights. While the GDPR protects people in the EU, the CCPA is specifically designed for California residents. According to a standardized regulatory impact assessment conducted by Berkeley Economic Counseling and Research, LLC, the CCPA regulations protect more than $12 billion worth of personal information used in advertising each year in California. Why is california consumer privacy law? California's Consumer Privacy Act aims to protect consumers' privacy for Californians in the same way that the GDPR protects Europeans. The CCPA may seem like a pain for companies, but it's a huge leap for consumers who value privacy. After all, we are all consumers and should care about the privacy of your personal information. So much of how we interact with businesses and organizations is now digital, we share and leave behind an incredible amount of personal data, often the data we don't even realize we have. Here's your information. It's yours. But so far, the entities that use the data have not been responsible for what they did to your data. CCPA aims to change this, creating new how their personal data is collected and used. Keep in mind that it's not just personal information, such as names and addresses. We're talking about... Credit Card Numbers Real Names Postal Addresses Social Security Numbers Demographic Data Income or similar information Browsing History and Search History Age Trading Information Policy Links Education Information Religions Relations Unique Personal ID/Account Name/Online ID Driver License Number Geolocation Data Biometric Data Biometric Data or Other Device Similar Identifiers Passport Number Other Identifiable Information This Personal Information Most People Do Not Notice Companies Collecting, Sharing and Selling. For the most part, this data is used to target marketing and advertising campaigns, but it also gets into the wrong hands to steal identities through data breaches. Either way, California's Consumer Privacy Act believes consumers should have certain rights and businesses have certain obligations. (You will notice that these rights reflect the GDPR). Because of this, the feet of the organisms are held to the fire. Undertakings must demonstrate that they are taking appropriate measures to either protect the data that consumers share with them or do not collect or share the personal data of consumers who refuse authorisation. The necessary measures in California's Consumer Privacy Act are lengthy and specific. If it wasn't, it would be too much to interpret. What are the rules in place in the new CCPA Privacy Act on personal data? Since the CCPA is relatively new, you can imagine questions constantly arise. Several proposed amendments to the original regulations have already been proposed. Companies should remember that these rules are quite fluid. Until these amendments are accepted, we can see what we know is currently in place. According to the California Office of the Attorney General, it remains CCPA-compliant for businesses: Notify consumers or before personal information is collected Allows consumers to opt-out, read, and delete personal information from their business storage. Companies must provide the Don't sell my personal information link to unsubscribe requests Reply to consumer requests within the timeframes set: Consumers' privacy settings indicate that they can be selected On-out is to verify the identity of consumers who request the reading and deletion of their data, even if they have a password-protected account to disclose the Company with financial incentives to preserve or sell the consumer's personal data, and how they assess the data, how they are introduced to register all access applications 24 and how the business response responded. What consumer rights does CCPA establish in respect of personal data? The CCPA creates specific consumer rights in terms of personal data and data protection. These rights are similar to those created by the GDPR, although they apply only to California residents. Residents residents the following new rights: Right to collect, use, share or sell personal data, both in categories and in respect of specific personal data The right to delete personal data held by businesses and their suppliers The right to opt out of the sale of their personal data and the company's instructions not to sell your data. Children under the age of 16 must give consent. Children under the age of 13 require the consent of the parent or guardian. The right to non-discrimination where the consumer exercises personal rights under the CCPA. Who should comply with the CCPA Data Protection Act? CCPA doesn't just apply to huge businesses like Google or Amazon. While all companies need to evaluate the privacy of their customers and visitors, not all businesses must comply with CCPA. California's attorney general has included rules exempting some businesses. CCPA only applies to the business if one or more of the following are true: There is a gross annual income of $25 million from buying, receiving, or selling the consumer's personal information to 50,000 or more consumers, households, or assets derived from 50 percent or more of the proceeds from the sale of consumers' personal information. In addition, businesses that process the personal data of more than 4 million consumers will have to pre-discover additional obligations. What happens if you don't comply with California's new privacy law? Fines for non-compliance with California's new privacy law depend on the offense and other factors. Civil penalties begin at $2,500 per violation, which is unintentional. Intentional non-compliance, these fines jump as much as $7,500 per violation. Then there's the timeframe in which the business responds. The CCPA states that if a company can cure a non-compliance within 30 days of being notified of the crime, it will get off with a warning. If they can't remedy the situation that fast, they can get back on the hook and make fines. Data breaches open a whole new wormbox, allowing affected consumers to take concrete action against the offiage company. Consumers can pay statutory compensation in the event of a data breach caused by the organisation's failure to implement reasonable security procedures for consumers' personal data. How will the California Attorney General enforce this new privacy law? California Attorney General Xavier Becerra still hasn't made plans for enforcement clear, even with all the publicity around the CCPA. The only thing we know is that the state is so far limited in its enforcement capabilities. California's attorney general's office does not have the resources to allow companies to comply with California law and handle non-complying cases. This for a reason, it's expected that some companies will simply take the chance to avoid the Attorney General's eyes. California residents don't companies to figure out how to comply with CCPA. There are already consumer class actions that go through the court system (on the civil side of the law, judging legal damages). Their results are still pending, but potential litigation proves one point: companies will not get away with non-complying, at least not without huge costs. Aside from financial penalties (this amounts to a portion of the organization's annual revenue), companies are interested in earning the trust of consumers who demand to put their privacy first. Consumers are becoming savvier, learning about their rights and requiring companies to adhere to CCPA compliance or suffer the consequences. Protecting consumers' privacy rights is the right thing to do, and now that California's new privacy law is in place, companies doing business with california business or its residents will be forced to comply, whether they want to or not. Do any other states besides California have a privacy law protecting personal information? That's a good question. Many believe that consumers' right to privacy is a federal right, not a state's decision. The Federal Data Protection Act would create a uniform standard for all companies (similar to how the GDPR works). When it comes to sharing personal data, there are no limits. Currently, however, only New York and California have privacy laws. Most of the companies affected by CCPA have more than California residents as customers and have already taken steps to protect consumer data worldwide because of CCPA. Once the consumer rights base is already there, it is just as easy to involve customers in the US and beyond. The essence of the regulation is the protection of consumer data and personal data, as well as the transparency of the collection, storage, use and sharing of data. While no other state has come as far as California's new privacy law, it will likely serve as a model that all states will issue regulations if the federal government does not enter into federal privacy law. It is said that the states of New York and Illinois will jump on board sometime in 2020 under their own consumer privacy laws. Who is responsible for ensuring ccpa compliance and personal data security in my company? CCPA compliance is an all-out thing. CEOs and CEOs often lead the charge, but because many other departments collect and use consumer data, everyone needs to understand the new data protection law and take responsibility for what they do with personal information. An example is marketing. Marketers consistently rely on consumer data to influence their campaigns. Consumer data is precisely what enables companies to make marketing efforts to the right people, to the right people to increase sales in a timely manner. Every time a consumer is tracked by a cookie on a website, he fills out a form or buys purchases personal data to the company, whether they recognize it or not. And according to the CCPA, that information is now protected by data protection laws. The same applies to the sales department. All customer data stored in systems such as Salesforce must be protected. If it is shared with other departments, these departments are owned. You can see how quickly and easily consumer data spreads ly ly through your body. Therefore, companies need to find a systematic way to comply with CCPA requirements. This means that all databases must be cleaned and reviewed so that the organisation can identify consent. This means that you place consent pop-ups and policies on your site. This means notifying consumers how consumers are collected, stored, used and shared. Proactive behaviour is the best way to minimize the risk of non-compliance. CCPA requirements go beyond their own four walls as well. Let's say your company shares customer information with other companies. In this case, your company must also demonstrate that it has taken appropriate measures to protect the data as soon as it is in their hands. The web of data sharing and the responsibility for data ownership are extensive, complex, and dynamic. Are there consent requirements for cookies in this new data protection law? We live in a world of cookies. Unfortunately, it's not the sweet kind. We are talking about the technical cookies on every website and the mobile application now uses to harvest personal information and learn about visitor habits. These cookies aren't that bad. They create a simpler user experience (for example, they remember what you put in your online shopping cart) and track consumers for marketing purposes. This is the latter reason why cookies are a cover point when it comes to California's consumer privacy law. The CCPA wants companies to be more transparent about how consumer data is collected and used, ensuring that consumers are aware that they are being used. If your website uses cookies, you should let visitors know. You can't hide your cookie policy in an ocean of legal jargon on a hard-to-find website. Companies should remember that the data collected by cookies is not theirs. It's the users, and they're the ones that control it. Cookie consent requirements mean that companies must use clear language in a clearly visible place to inform visitors about their cookie policies before collecting data. Visitors should be able to accept or reject the terms. You've probably seen pop-up boxes when you landed on websites. It's up to the company to make these pop-up boxes sued and visiting Track. You must disclose that you use cookies, tell us why you use them and allow visitors to give their consent or refuse. If the visitor opts out and refuses to use cookies, he or she must be able to block cookies and record the visitor's choice. What about the cookies I need? According to all of this, CCPA CCPA the necessary cookies (the so-called basic cookies in this Privacy Act). These are cookies that perform basic functions for the functioning of the website, such as accessing the password-protected part of the website or remembering the products of the shopping cart. If these necessary cookies are placed directly by an enterprise, CCPA does not require businesses to provide consumers with the opportunity to turn them off. Does the California Data Protection Act set out privacy policies? As well as the consent of cookies (as shown in the GDPR Data Protection Act), ccpa requires companies to do so in accordance with their privacy policies. As most consumers are unclear about the purpose of the data protection directives, companies need to define them accurately. Consumers are not alone in their insecurity. Unfortunately, many companies are not necessarily clear about how they handle consumer data and how they respond to data breaches, especially if they have transferred this personal information to suppliers and other third parties who may use this data themselves. Complicating things, privacy policy laws vary from state to state and often change. Most companies don't have the resources to track it all, much less ensure that they adhere to the CCPA guidelines. The CCPA requires that specific information be included in the Privacy Policy and must be updated annually. As with the consent of cookies, consumers should be notified that they are collecting their personal data and the reason for it. You'll then be given the option to accept or reject it - and that includes third-party cookies that can be embedded on your website. You need to track users' preferences, even if you're not entirely sure what they're collecting or who's collecting. Is there an easy way to comply with California's new privacy law? I'm glad you asked. Yes, there is. California's new data protection law simply contains guidelines and penalties for non-compliance. The measures taken by the company to comply with the law depend on them. You can choose to manually write, encode pop-up approval fields, track consumer preferences, and manage the use of shared data by vendors, or automate them. A single line of JavaScript on its website immediately complies with data protection laws (including the GDPR and the California Consumer Privacy Act), even if you use third-party cookies, share consumer information with companies in other states or countries, or if privacy laws change. All consents and withdrawals are recorded and searched with one click for responsible data management. There are also free and open source sources make cookies notices and categories of personal information in the wind. Again, it uses automation to easily manage consents, even change the visitor's language, and then track contributions to auditable records. When it comes to vendors, do you know what they do with the personal information customers and users have shared with them? If you don't want to offend new data protection law, you should know. Depending on your vendors, this task is virtually impossible because most vendors do not reveal how this information is used or shared. You may not use CCPA to share or sell your consumer data to suppliers or third parties, or to do so. It is your responsibility to keep consumers' personal data safe and to comply with their wishes for the use of their data. As you continue to own consumer data, it's important to partner with manufacturers who share your commitment to protect consumer data and comply with California's Consumer Privacy Act. You'll know this if you're automating how you can monitor privacy practices among current and prospective vendors. Osano's automated solution is able to combine legal experts and AI technology to sift through any legal jargon to de-line exactly how each manufacturer handles consumer data and gives each seller a risk score. You can also see how vendors and vendor vendors handle this data - all with one click. This is a quick and easy way to evaluate suppliers and ensure that they do their best to protect the personal information they share with them. This proves valuable in the event that it is audited. Adhere to California's Consumer Privacy Act for greater good data protection than saying, it's not a question of if, but when. California's Consumer Privacy Act is a good thing, and it's very likely several states will draft their own privacy laws in the near future. The sooner you jump the company on board, prioritize your initiative, and putting mechanisms in place to support it, the sooner you can move forward with confidence in what contributes to the greater good. Good.