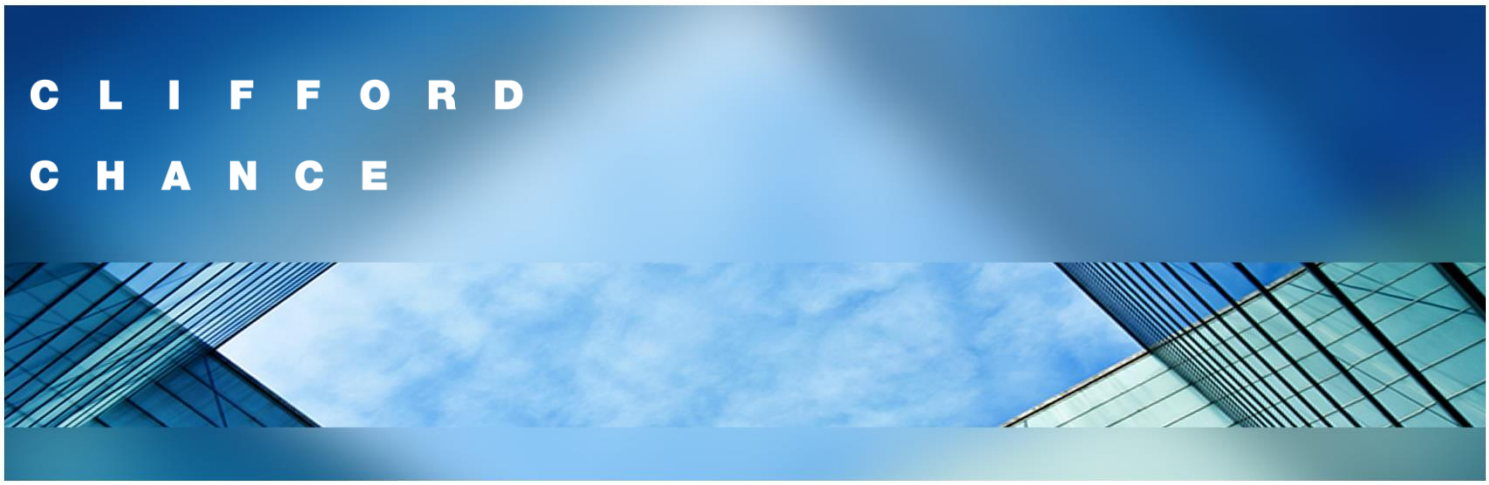

CALIFORNIA'S NEW DATA PRIVACY LAW: IMPLICATIONS FOR ASSET MANAGERS

The recently enacted California Consumer Privacy Act of 2018 (the "California Privacy Act" or the "Act")[1], will require companies that do business in California to provide notice regarding the collection and use of personal information, delete personal information upon request, allow individuals to opt out of the sale of their personal information, and adopt reasonable security procedures and practices to protect personal information. The Act will protect a far broader category of "personal information" than is covered by most other state and federal statutes, will provide enhanced penalties for noncompliance, and will provide a private right of action. The Act will become effective in January 2020 unless it is amended beforehand.

The Act addresses many of the same privacy and security concerns as the European Union's General Data Protection Regulation (GDPR) but is distinct in several key respects. Asset managers doing business in California will likely be subject to the Act and should evaluate their privacy practices accordingly.

THE CALIFORNIA CONSUMER PRIVACY ACT OF 2018 EXPLAINED

The Act's Broad Application

The Act applies broadly to businesses that participate in the collection of personal information and which meet any one of three standards: (i) "annual gross revenue in excess of twenty-five million dollars"; (ii) "alone or in combination, annually buys, receives for the business' commercial purposes, sells, or shares for commercial purposes, the personal information of 50,000 or more consumers, households, or devices; or (iii) "derives 50 percent or more of its annual revenues from selling consumers' personal information." Pursuant to the Act, any affiliates or

[1] To be codified at CAL. CIVIL § 1798.100 effective January 1, 2020.

subsidiaries of a business that fall within one of these categories will also be subject to the Act if it "shares common branding with the business."

A business does not need to have a physical presence in California for the Act to apply. The Act applies to 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 does business in the State of California" and is involved in the collection of personal information belonging to natural persons who are residents of California.

An Expanded Definition of Personal Information

Prior to the passage of the California Privacy Act, California data protection laws only applied to a relatively narrow class of "Personal Information," which included an individual's name in conjunction with information such as a social security number, driver's license number, financial information, and medical information. This definition was in-line with standards in most other states.

The California Privacy Act adopts a more expansive definition of personal information. Under the Act, "personal information" 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." The Act also identifies specific examples of personal information, including, but not limited to commercial information, biometric information, internet or other electronic network activity information, geolocation data, audio, electronic, visual, thermal, olfactory, or similar information, professional or employment-related information, and education information.

The Act's Affirmative Requirements

Businesses subject to the Act also have specific obligations. These include:

- A duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.[2]
- A duty to notify individuals of the categories of personal information to be collected and the purposes for which the categories of personal information will be used, as well as a duty to provide additional notice before the collection of additional categories of personal information.
- A requirement to provide notice to individuals that their information may be sold and that they have the right to opt out of the sale of their personal information.
- A prohibition from selling the personal information of individuals if the business has actual knowledge that the individual is less than 16 years of age, unless the individual, in the case of a person between 13 and 16 years of age, or the

[2] With respect to this provision, the Act uses a narrower (and more conventional) definition of personal information as "(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, or password that would permit access to an individual's financial account. (iv) Medical information. (v) Health insurance information. (B) A username or email address in combination with a password or security question and answer that would permit access to an online account." CAL. CIVIL § 1798.81.5.

person's parent or guardian, in the case of individuals who are less than 13 years of age, has provided affirmative authorization.

- A prohibition from discriminating against a person because that person exercises any of their rights under the Act. Nonetheless, a business may offer financial incentives for the collection, sale, or deletion of personal information. However, the financial inventive may not be unjust, unreasonable, coercive, or usurious. The Act states that discrimination against a consumer includes, but is not limited to, denying goods or services to the consumer, charging different prices or rates for goods or services, providing a different level or quality of goods or services to the consumer, and 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.
- A requirement to make available to individuals 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 a web site, a web site address. A business must disclose and deliver the requested information to a consumer free of charge within 45 days of receiving a verifiable request from the consumer. Additionally, a business that sells personal information must provide a clear and conspicuous link on the business' homepage, titled "Do Not Sell My Personal Information," to a web page enabling an individual to opt out of the sale of personal information.
- A requirement to disclose information regarding an individual's rights under the Act and list categories of personal information it has collected over the previous 12 months. The business must disclose this information in its online privacy policy and in any California-specific description of consumers' privacy rights (or if it does not maintain an online privacy policy, it must disclose the information on its website). In addition, a business must ensure that all individuals responsible for handling inquiries about the business' privacy practices or the business' compliance with the Act are informed of its requirements and how to direct customers to exercise their rights.

New Rights and Penalties Created by the California Privacy Act

The California Privacy Act also gives individuals specific rights over their data. These include the right:

- To request that a business delete personal information about the individual which the business has collected from the individual;
- To request that a business that collects or sells personal information disclose the categories of personal information, the sources from which such personal information is collected, the business or commercial purpose for collecting or selling personal information, the categories of third parties with whom the business shares personal information, and the specific pieces of personal information it has collected about that individual.
- To direct a business that sells personal information to third parties not to sell the individual's personal information.

Enforcement Rights

The California Privacy Act also gives both individuals and the California State Attorney General tools to enforce the statute. *First*, the California Attorney General will have the authority to bring enforcement actions for any violations of the Act. Following the initiation of an enforcement action, a business will be given 30 days to cure any alleged violation of the Act. Failure to do so can result in penalties of up to $7,500 for each intentional violation or $2,500 for each unintentional violation.

Second, individuals or classes of individuals can bring a civil action against a business if their unencrypted personal information is subject to unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices.[3] In the event of a breach, each individual has the right to seek damages of up to $750 per person per incident or actual damages (whichever is greater), injunctive or declaratory relief, or any other relief the court deems proper.

However, a claimant seeking the $750 statutory damages must provide the defendant with 30 days' notice of the suit, during which time the business may provide written notice demonstrating that the violation has been cured and will not recur. Potential claimants must also provide notice of the suit to the Attorney General and the Attorney General can take over the action, order the consumer not to prosecute the action, or allow the suit to proceed.

Overlap with the GDPR

While there is overlap between the California Privacy Act and the GDPR, such as requiring disclosure regarding the uses of personal information, the adoption of adequate security measures and the creation of certain enumerated privacy-related rights, the two regimes contain material differences. For example, the Act contains requirements not found in the GDPR, such as the creation of specific mechanisms for individuals to submit requests regarding their data, a requirement to make certain disclosures available on a business' website, and the requirement for businesses that sell personal information to develop a "Do Not Sell My Information" web portal. The definition of personal information also differs from that employed by the GDPR. Lastly, some entities not subject to GDPR will be subject to the Act, and vice versa. Therefore, while GDPR compliant businesses will have a head start regarding implementation of the California requirements, they will still need to monitor the adoption and possible amendment of the Act and evaluate their data privacy practices prior to January 1, 2020.

Implications for Asset Managers

Asset managers should take note of the new California legislation and begin to prepare for its January 1, 2020 effective date. Pursuant to the Act, asset managers with annual revenues over $25 million and who do business with investors, employees or other third parties in California will likely be subject to the Act and its requirements. To prepare for the Act's effective date, asset managers should consider taking the following steps:

---

[3] With respect to this provision, the legislation uses the narrower definition of personal information set forth in CAL. CIVIL § 1798.81.5.

- **Evaluate Security Procedures and Practices:** Asset managers should evaluate their security procedures and practices to ensure they are "reasonable" and "appropriate" with respect to the nature of the information held.
- **Inventory Personal Information:** While the Act requires individuals to affirmatively request disclosure of their personal information, businesses must comply within 45 days of receiving such a request and must maintain up to date notices regarding information collection. Therefore, asset managers should undertake an inventory of personal information in their possession to comply with requests in a timely manner and maintain current disclosures. Asset managers should also be cognizant of the sale or transfer of personal information to third parties, including vendors, which may impact disclosure obligations per an individual's request.
- **Crafting Disclosures:** Asset managers will be obligated to inform individuals as to the categories of personal information that will be collected and the purposes for which such information will be used. Furthermore, the transfer or sale of assets that hold personal information may trigger disclosure requirements to individuals regarding the change in control of their personal information.
- **Providing Mechanisms for Submission of Requests:** Asset managers will be required to make available to individuals two or more designated methods for submitting requests to exercise their privacy-related rights. Additionally, to the extent that an asset manager is engaged in the sale of personal information, it will be required to implement the "Do Not Sell My Personal Information" web page to enable individuals to opt out of the sale of their personal information.
- **Employee Training:** While the Act does not explicitly require the designation of a data protection officer, it does suggest that businesses, including asset managers, will have to ensure employees are informed of these obligations and how to direct individuals in exercising their rights.

CONTACTS

Daniel Silver
Partner

T +1 212 878 4919
E daniel.silver
@cliffordchance.com

Megan Gordon
Partner

T +1 202 912 5021
E megan.gordon
@cliffordchance.com

Benjamin Berringer
Associate

T +1 212 878 3372
E benjamin.berringer
@cliffordchance.com

Daniel Podair
Associate

T +1 212 878 4989
E daniel.podair
@cliffordchance.com

www.cliffordchance.com

Clifford Chance, 31 West 52nd Street, New York, NY 10019-6131, USA

Clifford Chance US LLP

Abu Dhabi • Amsterdam • Barcelona • Beijing • Brussels • Bucharest • Casablanca • Dubai • Düsseldorf • Frankfurt • Hong Kong • Istanbul • London • Luxembourg • Madrid • Milan • Moscow • Munich • Newcastle • New York • Paris • Perth • Prague • Rome • São Paulo • Seoul • Shanghai • Singapore • Sydney • Tokyo • Warsaw • Washington, D.C.

Clifford Chance has a co-operation agreement with Abuhimed Alsheikh Alhagbani Law Firm in Riyadh.

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.