

# The GDPR Was Just the Beginning

Companies that process personal data of California residents will soon be subject to comprehensive new privacy requirements.

**By: Jacqueline Klosek**

Just as those of us in the privacy field had begun to have a slight breather as much of the heavy lifting on the European General Data Protection Regulation (GDPR) was finally behind us, lawmakers in California passed the **California Consumer Privacy Act of 2018** (CCPA). The CCPA, effective as of Jan. 1, 2020, will require companies, wherever located in the world, that process the personal data of residents of California to observe restrictions on data monetization, provide for data subject rights that are similar to those found in the GDPR, update their privacy policies and to take steps to protect against the possibility of penalties and liquidated damages.

## Scope

The CCPA will apply to all companies, wherever located, that receive personal data from California residents if they or their parent company or a subsidiary:

(a) Have annual gross revenues in excess of \$25 million;

(b) Obtain personal information of 50,000 or more California residents, households or devices annually; or

(c) Obtains 50 percent or more annual revenue from selling California residents' personal information.

The CCPA defines personal information very broadly, expanding the existing definition to include any data that relates to or can be associated with a particular consumer, including contact information; online identifiers; government ID numbers; purchase history and other commercial data; biometric information; browsing/search history; sensory, geolocation, professional, employment, or education data; and any data used "to create a profile reflecting preferences, characteristics, ... behavior, attitudes, intelligence, abilities, and aptitudes." Given the very broad definition of "personal information," the CCPA will have a profound effect on technology companies whose operations involve the processing of data.

## New Rights for California Residents

Like the GDPR, the CCPA provides data subjects with a number of privacy rights, including:

- **Rights of access and knowledge:** Once the CCPA is in effect,



**Jacqueline Klosek, Goodwin counsel.**

California residents will have the right to access and know what personal information is collected. Prior to collection, companies must make a number of mandatory disclosures, including the categories and uses of personal information in transactional and other contexts. California residents will also have the right to know whether personal information is sold or disclosed and to whom. Companies must inform requesting consumers about the categories of

personal data sold to third parties or disclosed in connection with a transaction. Third-party recipients of personal information are prohibited from selling the data without notice and an opt-out.

- **The right to object:** Upon request, companies must stop selling personal information. In addition, companies wishing to sell personal information from children will be required to obtain opt-in consent from the child if the child is 13 to 16 years old or from the child's parent or guardian if the child is younger than 13.

- **The right to deletion:** Subject to certain exceptions, a company that receives a deletion request from a consumer must erase the consumer's personal information from its systems and must also direct its service providers to do the same. As with the GDPR, this will require companies that are in control of personal information processing operations to enter into agreements with their service providers so as to ensure they will be able to comply.

- **The right to be free from discrimination:** The CCPA prohibits its companies from discriminating against consumers who exercise their CCPA rights.

### Enforcement

The CCPA creates a private right of action with the potential to recover damages of \$100 to \$750 for each affected consumer, exposing companies to an enhanced risk of class actions and costly litigation. In addition, companies will violate the CCPA if they fail to cure within 30 days of receiving notice from the AG. Such

violations will be subject to civil penalties of up to \$2,500 per violation. Intentional violations can result in civil penalties of up to \$7,500 per violation. The AG could seek to multiply penalties by the number of affected consumers and/or the number of days the violation occurred.

### Preparing for the CCPA

Companies that will be subject to the CCPA are advised to act promptly to assess the new law's impact on their business and develop a compliance roadmap. Although compliance is not required until January 2020, as anyone who has been working on GDPR compliance knows all too well, implementing compliance programs for major legislative changes does take a significant amount of time. Here are some concrete steps to take right now:

- **Assess data practices:** If not already done recently in connection with GDPR compliances, companies to be subject to the CCPA should consider mapping current data flows and privacy practices.

- **Analyze compliance gaps and begin to make necessary changes:** Make available designated methods for submitting data access requests, including, at a minimum, a toll-free telephone number. Provide a clear and conspicuous "Do Not Sell My Personal Information" link on the business' internet homepage that will direct users to a web page enabling them, or someone they authorize, to opt out of the sale of the resident's personal information. Companies should also consider reviewing vendor agreements to determine if they

need to be renegotiated to address the forthcoming changes in law.

- **Update privacy policies:** The CCPA will mandate a number of additional disclosures beyond what are typically included in most privacy policies today. To prepare for the entry into force of the CCPA, companies should begin to evaluate the changes that they will need to make to their policies and begin to modify their policies.

- **Stay up to date on future legal developments:** The CCPA requires the AG to solicit public participation to adopt regulations to further the purposes of the [CCPA], including the establishment of possible exceptions. As such, attention will need to be directed to the evolving regulatory landscape.

*Jacqueline Klosek is a counsel in Goodwin business law department and a member of its intellectual property group as well as its privacy and cybersecurity practice. Her practice focuses on transactions involving technology and intellectual property, and she regularly advises clients on various issues related to privacy and data security. She is a key contributor to Goodwin's Founders Workbench, an online resource for startups, emerging companies and the entrepreneurial community. Klosek drafts and negotiates various technology agreements and advises on different aspects of the law related to intellectual property and technology. She also advises clients on various issues related to privacy and data security.*