



DECEMBER 11, 2019

CALIFORNIA CONSUMER PRIVACY ACT EMPLOYMENT MORATORIUM ALERT

In concluding the legislative session for 2019, the California State Legislature passed a variety of amendments to the California Consumer Privacy Act (Cal. Civ. Code § 1798.100, *et seq.*) (“CCPA”). Among the five substantive amendments sent to Governor Newsom for approval, AB 25 is of particular importance for employers. While AB 25 provides some, albeit temporary, relief with respect to personal information about employees, it does not fully relieve employers of all CCPA compliance obligations with regard to employees, job applicants, and other similarly situated individuals. Accordingly, there is still work to be done before January 1, 2020 and beyond.

Structurally, AB 25 alters the CCPA’s definition of “personal information” to exclude information collected “about a natural person acting as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or contractor of [a covered] business” to the extent the covered business’ collection and use of such information is done solely within the context of the natural person’s role with the business. The exclusion also extends to emergency contact and benefit administration information.

In altering the definition of personal information, AB 25 limits businesses’ compliance obligations. Specifically, businesses will not need to facilitate any CCPA rights for disclosure, deletion and opt-out made by individuals with respect to the information described above until 2021. However, the moratorium stops far short of what employers were hoping for by leaving the compliance obligations and risk untouched, as summarized below.

Employee Notice Obligations Remain

- Starting January 1, 2020, businesses are still obligated to render all CCPA compliant notices at the point of collection on or before January 1, 2020, to all employees, job applicants, contractors, directors, medical staff members, or officers. Accordingly, businesses must describe to these individuals what categories of personal information will be collected and the purposes governing collection.

Information Security Risk for Employment Data Remains

- Additionally, AB 25 does not limit business exposure from private rights of action or class litigation. In instances involving a data breach where a business has not implemented reasonable security measures, employees alongside other consumers are permitted to seek and recover statutory damages between \$100 and \$750 per incident.

Employee Data Used for Multiple Purposes Not Exempt

- Finally, employers must review their information practices to determine whether any personal information collected from employees, job applicants, and other similar individuals is used or shared for any purposes other than exclusively employment purposes. Such use cases will fall outside the scope of the AB 25 moratorium and therefore trigger the obligation for full CCPA compliance with respect to such information and practices. For example, making any transfers of employee-related data that meet the CCPA’s board definition of sale (i.e., any disclosure to a third party for monetary or “other valuable consideration”) would almost certainly not be considered as being done “solely” within the context of the employee’s roles within the business, and, therefore would trigger the CCPA’s opt-out and other sale disclosure requirements.

The moratorium created by AB 25 is set to expire on January 1, 2021. The California State Legislature is expected to either remove, extend, or make the moratorium a permanent provision within the CCPA. Alternately, the Legislature may enact separate legislation and corresponding regulations addressing personal information within the employment context. In

the meantime, businesses should continue to develop public-facing policies and internal procedures to implement the requirements contained within the CCPA and the recently released Proposed Text of Regulations (Cal. Civ. Code § 999.300, *et seq.*).

While January 1, 2020 is just around the corner, many businesses will continue to assess and remediate their CCPA compliance gaps into the new year. This is understandable given the complexity of the law, the myriad of drafting issues stemming from the haste with which the law was passed, the yet to be finalized Attorney General implementing regulations (California Civil Code § 999.300, *et seq.*), and the drain on internal resources typically required to address CCPA compliance. Nevertheless, as a reminder, while the California Attorney General will not be permitted to initiate CCPA enforcement actions until July 2021, it will be able to pursue earlier violations at that time.

Kutak Rock's [Privacy and Data Security Group](#) is ready to help your company understand and implement all necessary CCPA compliance measures.

Contacts			
Jon Breyer	Minneapolis	(612) 334-5057	Jon.Breyer@KutakRock.com
Nicole Moriarty	Washington, D.C.	(202) 828-2446	Nicole.Moriarty@KutakRock.com
Todd Kinney	Omaha	(402) 231-8968	Todd.Kinney@KutakRock.com
Jacob Tewes	Omaha	(402) 661-8611	Jacob.Tewes@KutakRock.com

This Privacy and Data Security Client Alert is a publication of Kutak Rock LLP. This publication is intended to notify our clients and friends of current events and provide general information about privacy and data security issues. This Kutak Rock LLP Privacy and Data Security Client Alert is not intended, nor should it be used, as specific legal advice, and it does not create an attorney-client relationship.

©Kutak Rock LLP 2019 – All Rights Reserved

This communication could be considered advertising in some jurisdictions.

The choice of a lawyer is an important decision and should not be based solely upon advertisements.