KUTAKROCK

April 8, 2019

Colorado Privacy Law Summary

On September 1, 2018, changes to Colorado's Consumer Protection Act (HB 18-1128, the "CPA") came into effect. This statute made significant changes to Colorado's data privacy laws that affect nearly all Colorado businesses and government entities. Its restructuring is an obvious and powerful assertion that public entities should take this statute and these responsibilities seriously.

Affected Entities

Before the CPA revisions, Colorado had a single set of data breach, data disposal, and security requirements for "public and private" entities under Title 6 (Consumer and Commercial Affairs) of the Colorado Revised Statutes. The revised provisions in Title 6 apply to "covered entities," i.e., persons or entities that maintain, own, or license personal information of Colorado residents in the course of their business, vocation, or occupation. The new statute also adds completely new sections in Title 24 (Government – State) that mirror Title 6 but apply to "governmental entities," which include the state; any state agency or institution; the judicial department; any county, city and county, incorporated city or town, school district, special improvement district, authority, or entity governed by home rule charters; and "every other kind of district, instrumentality, or political subdivision of the state organized pursuant to law." Either type of entity is deemed to be in compliance with the CPA's breach notification, security policy, and disposal policy requirements if it is regulated by another state or federal law and protects the relevant personal information or personal identifying information according to those obligations, except that it still must notify the Colorado Attorney General for large breaches.

Breach Notification Requirements

Like most data breach statutes, the CPA defines "personal information" as a Colorado resident's first name or first initial and last name in combination with certain data points specified in the law, such as a social security number or medical information. A username, email address, account number, or payment card number in combination with its password or access code also qualifies as personal information. The definitions for "personal information" and "security breach" each have an exception for encrypted data, which effectively means encrypted data are not subject to the CPA unless the decryption key is also compromised. Once a covered or governmental entity becomes aware that a security breach *may have* occurred, it must investigate and determine whether it is reasonably likely that personal information has been or will be misused. If not, there are no notice obligations. If so, the entity must give notice within thirty days after "the point in time at which there is sufficient evidence to conclude that a security breach has taken place." Additionally, if the entity determines that a username or email address has been lost in conjunction with the password or other credentials needed to access an online account, the entity must send *another* notice directing the recipient to change his or her account information and take certain other steps. The CPA also requires entities to notify the Colorado Attorney General and the major consumer reporting agencies if the Colorado recipients number more than 500 or 1,000, respectively.

Data Disposal and Security Policies

In addition to notification requirements, the CPA requires covered and governmental entities (as well as their third-party service providers) to implement and maintain written policies for disposal of paper and electronic

documents containing "personal identifying information" and to implement reasonable and appropriate security procedures and practices. Documents that contain "personal identifying information" must be destroyed, erased, or made unreadable as soon as they are no longer needed unless otherwise required by law. Unlike the definition of personal information, the definition of personal identifying information does not require an individual's name and excludes medical information or health insurance identification numbers. This means that, for example, a lone social security number that is not accompanied by a name would qualify as personal identifying information but not as personal information.

Enforcement

The CPA gives the Colorado Attorney General the authority to use actions for injunctive relief against governmental entities and actions for either injunctive relief or damages against a covered entity to enforce the CPA. The CPA does not create a new private right of action, but whether violations of this statute could qualify as a deceptive trade practice and trigger a private right of action under other portions of the Consumer Protection Act remains to be seen. With approval from the governor or a district attorney, the Attorney General can also prosecute criminal cases related to a reported security breach for violations of Colorado's cybercrime statute.

Third-Party Service Providers

Third-party service providers that maintain, store, or process personal information on behalf of a covered or governmental entity have their own set of obligations under the CPA. They must notify their respective entities in the event of a security breach "in the most expedient time possible and without unreasonable delay . . . if misuse of personal information about a Colorado resident occurred or is likely to occur." The construction of the CPA suggests but does not expressly state that the third-party service provider is to make that determination. The CPA also requires covered and governmental entities to pass the CPA's security policy requirements (with certain exceptions) through to those entities' third-party service providers.

Conclusion

The revised CPA affects public and private entities at all phases of the data protection life cycle. Affected companies, governmental agencies, and others should evaluate their security programs, data disposal policies, and incident response plans for compliance with these stringent obligations. Kutak Rock's Privacy and Data Security team stands ready to assist with these and other issues in this constantly shifting landscape.

Contacts			
Jon Breyer	Minneapolis	(612) 334-5057	Jon.Breyer@KutakRock.com
Robert Grennan	Omaha	(402) 231-8856	Robert.Grennan@KutakRock.com
Todd Kinney	Omaha	(402) 231-8968	Todd.Kinney@KutakRock.com
Nicole Moriarty	Washington, D.C.	(202) 828-2446	Nicole.Moriarty@KutakRock.com
Jacob Tewes	Omaha	(402) 661-8611	Jacob.Tewes@KutakRock.com