What To Know About New Colo. Data Privacy Law

Law360, (June 14, 2018)

Erin Eiselein

Esteban M. Morin

Anna-Liisa Mullis

In late May, Colorado enacted a sweeping new data security law that will impact businesses throughout the country. The new law — HB 18-1128, or the data security law — imposes several requirements on companies that maintain the personal information of Colorado residents. Specifically, the data security law establishes new obligations regarding: (1) data breach response; (2) the protection of certain types of personal information; and (3) the disposal of certain types of personal information, although the third obligation applies only to companies with a physical presence in the state. On their face, these new requirements apply to most companies that collect personal information online and establish Colorado as one of the most aggressive states in the nation with regard to data security.

Although the data security law does not go into effect until Sept. 1, 2018, companies should begin preparing for it well before that date. Many entities will need to engage in internal security audits and modify their existing policies to ensure compliance with the new requirements. To facilitate this process, companies should consider devising a formal compliance plan. By following such a plan, companies in all industries can use the new law as an opportunity to improve their data security practices and better protect Colorado residents' confidential information.

Overview of the Data Security Law

The data security law modifies and supplements existing privacy and security laws in a number of ways. These changes generally result in a set of obligations that are more expansive and stringent than their predecessors. For example, the new law defines "personal information" to include a Colorado resident's first name or first initial and last name in combination with another piece of information such as the individual's identification number (including Social Security, driver's license and passport numbers), medical information or biometric data. These last two categories are new additions and expand the meaning of personal information beyond the definition utilized by many states. The definition also includes a Colorado resident's email address, account information or credit card number in combination with a password or security.

In addition to utilizing a broad definition of personal information, the data security law imposes its requirements on any entity that "maintains, owns or licenses personal identifying information in the course of ... business." These "covered entities" include businesses and nonprofit entities in all industries as long as they store at least one piece of personal information from a Colorado resident. As such, any private entity that has any customers, donors, patients, affiliates or vendors in Colorado is likely subject to certain provisions of the data security law. The data security law also imposes comparable requirements on governmental entities

in Colorado that maintain, own or license personal information concerning Colorado residents.

As noted above, there are three different types of obligations imposed by the new law. Closely examining each of these in turn provides insight into the impact of each requirement and what steps covered entities can take to ensure compliance.

New Data Breach Reporting Obligations

The most far-reaching requirements in the data security law relate to data breach notification. Although Colorado previously required companies that conducted business in the state to provide notice to affected state residents as soon as possible after discovering a breach, the new law imposes two significant new requirements. Most significantly, an entity that suffers a breach that implicates the personal information of Colorado residents must now provide notice to affected individuals within 30 days. Additionally, if the breach implicates at least 500 Colorado residents, the entity must also provide notice to the Colorado attorney general within 30 days. These requirements put Colorado into a very small category of states that set express time limits on providing breach notifications and create a reporting regime that is more stringent than that of virtually any other jurisdiction outside the European Union.

Covered entities that suffer a breach are also required to include specific details in their breach notifications. The data security law requires that notice to Colorado residents include: (1) the date of the breach; (2) a description of the personal information required; (3) contact information for the entity; (4) information for contacting credit reporting agencies and the Federal Trade Commission; (5) information about receiving fraud alerts and freezing credit; and (6) if a username and password were compromised, a statement directing individuals to change their password and take other steps. Coupled with the 30-day deadlines, the new content requirements establish Colorado as one of the most prescriptive states in the country and make it more difficult for national or international companies to take a uniform approach when responding to data breaches.

New Data Protection Obligations

Colorado's new data protection obligations apply to the same set of covered entities as the breach reporting requirements, but only implicate a subset of personal information. This subset is labeled as "personal identifying information," and includes an individual's identification number (including Social Security, driver's license and passport numbers), biometric data and password. Under the data security law, any covered entity that maintains, owns or licenses personal identifying information from a Colorado resident must protect such information. Specifically, covered entities are required to "implement and maintain reasonable security procedures and practices that are appropriate to the nature of the ... information and the nature and size of the business." The data security law further requires that if it discloses personal identifying information to a third party, it must ensure that the third party reasonably protects the information. Finally, the data security law provides that companies that are already regulated by state or federal law and that maintain procedures for data protection pursuant to those laws are deemed in compliance with these new data security law obligations. To the extent companies are not deemed in compliance,

they will need to implement procedures and revise their third-party contracts to specifically address this issue.

The vague language used in the data protection provisions means that an entity's obligations will change over time. By design, the requirements will become more stringent as industry standard security measures evolve and companies expand their businesses to collect more information or more sensitive personal details from Colorado residents. This is a common trend in modern data security laws. For example, European regulators have similarly emphasized the importance of proportional and evolving data protection standards when discussing the enforcement of the General Data Protection Regulations, or GDPR.

New Information Disposal Obligations

The final set of requirements under the data security law is also the most limited in its application. Unlike the other new provisions, the data disposal requirements only apply to covered entities located within Colorado that maintain a subset of personal information — personal identifying information, discussed above. Colorado covered entities that maintain personal identifying information are required to develop a written policy for destruction or proper disposal of such information regardless of whether it is contained in paper or digital documents. Although no specific timelines for disposal are included in the law, it is implied that sensitive information should be disposed of when it is "no longer needed." Finally, the data security law provides that companies that are already regulated by state or federal law and that maintain procedures for data disposal pursuant to those laws are deemed in compliance with these new data security law obligations.

These requirements will apply to virtually all companies that have any physical presence in Colorado if they maintain human resources information, IT account data, biometric data (such as fingerprints), and a variety of other information. National or international companies with a Colorado outpost that are not in compliance will thus need to evaluate whether to modify their existing policies or create a set of Colorado-specific policies.

Enforcement

The Colorado attorney general may bring an action to address violations of the data security law's new breach reporting, data disposal and security requirements and may enforce compliance, recover damages resulting from a violation, or both. The data security law also gives district attorneys the authority to prosecute criminal violations amounting to computer crime.

Although the new data security law provisions are part of the Colorado Consumer Protection Act, or CCPA, which provides a private cause of action in connection with certain "deceptive trade practices," it is unclear whether violations of the data security law would give rise to a private cause of action under the CCPA. If a violation of the data security law is interpreted to be a deceptive trade practice subject to the CCPA, a successful plaintiff could potentially recover treble damages and reasonable attorneys' fees from a private entity subject to the data security law.

How to Prepare

The first step to complying with the data security law is to evaluate existing policies. It is especially important for entities to determine whether their existing breach response plans, information security policies, and (if applicable) data retention and disposal policies are sufficient. In all likelihood, covered entities will have to make changes to accommodate the new 30-day breach notice requirement and change their breach notice templates to include the specific content required by Colorado. It is likewise important for covered entities to verify that their information security policies provide reasonable, industry-standard technical, physical and administrative safeguards for personal information. In addition to these safeguards, covered entities should conduct regular audits of their security programs to ensure safeguards are up to date and adequate in light of the scope of sensitivity and amount of information that the entity is collecting.

For many companies, it is helpful to develop a comprehensive compliance plan that focuses on the entity's breach response, data protection and data disposal policies and practices. This plan should provide assurances that each topic is analyzed and addressed in a timely manner with minimal disruption. A compliance plan also can help identify overlapping obligations and allow an entity to address issues in a more streamlined manner. For example, by creating a plan, an entity may recognize that it can incorporate updates to its breach response plan that address both the 30-day reporting requirement under the data security law as well as the 72-hour reporting requirement under the GDPR, if applicable. Likewise, a compliance plan can align an evaluation of a covered entity's data protection policies for compliance with the new Colorado law with a preplanned security audit, and thereby avoid going through the same process twice.

The data security law will affect most, if not all, private companies and governmental entities in the state of Colorado and any national or international entity that maintains personal information of Colorado residents. Those private companies and governmental entities that have not previously needed to develop policies and procedures to handle breach reporting, data protection and information disposal will need to do so in order to comply with the new law. Because the compliance deadline of Sept. 1, 2018, is less than three months away, all companies covered by the law would do well to begin developing compliance programs, or reviewing and revising existing compliance programs, now.

Erin M. Eiselein is a shareholder and Esteban M. Morin and Anna-Liisa Mullis are associates at Brownstein Hyatt Farber Schreck LLP.