EMPLOYERS CAN PREPARE FOR NEW COLO. DATA PRIVACY LAW

By Dustin Berger

Republished with permission, this article first appeared in Law360, July 19, 2018.


Dustin Berger

Organizations that employ workers in Colorado will soon face more stringent data privacy requirements, thanks to new legislation signed into law by Gov. John Hickenlooper at the end of May. This new law, HB 18-1128, imposes new obligations on all covered entities in the state that maintain documents that contain personal identifying information of Colorado residents. These obligations go into effect on Sept. 1, 2018. Here are the highlights of the new requirements and steps employers should take to comply.

Practically All Employers Will Be Affected by the New Law

The new law applies to a "covered entity," which is essentially defined as any individual or entity "that maintains, owns or licenses personal identifying information" — regardless of how much business the covered entity does within Colorado. The statute defines "personal identifying information" as "a Social Security number; a personal identification number; a password; a pass code; an official state or government-issued driver's license or identification card number; a government passport number; biometric data; an employer, student or military identification number; or a financial transaction device."

Because virtually all employers maintain information on their employees that is considered personal identifying information, such as Social Security numbers, employer identification numbers, passport numbers or driver's license numbers, employers with Colorado employees will be subject to the requirements of the new law.

The key provisions in the new law are its requirements that covered entities: (1) maintain reasonable security procedures and practices; (2) establish and follow a written policy for the destruction of personal information when it is no longer needed; (3) ensure that third-party service providers handling their personal information have implemented and maintained reasonable security procedures and practices; and (4) follow the law's notification procedures when it becomes aware that a security breach "may have" occurred.

1. Reasonable Security Procedures and Practices

HB 18-1128 creates a new statutory section, C.R.S. § 6-1-713.5, that requires covered entities to implement and maintain reasonable security procedures and practices to protect personal identifying information from unauthorized access, use, modification, disclosure or destruction. While not specifying exactly what type of security procedures are required, the new provision states that such procedures must be appropriate to the nature of the personal identifying information and the nature and size of the business and its operations.

If a covered entity discloses personal identifying information to a third-party service provider, it must require that the service provider implement and maintain reasonable security procedures and practices, as outlined in number three below.

2. Disposal of Documents Containing Personal Identifying Information

Colorado has had a statute governing the disposal of documents containing personal identifying information since 2004, but the new legislation amends C.R.S. § 6-1-713 to expand covered entities' responsibilities with respect to personal identifying information. Now, the disposal requirements apply to documents that are kept electronically as well as those kept in paper form. The new law also requires that covered entities implement a written policy specifying that the entity shall destroy (or arrange for destruction of) the documents by making the information unreadable or completely indecipherable.

3. Ensure Third-Party Service Providers Have Reasonable Security Procedures

If a covered entity discloses personal identifying information to a third-party service provider, the covered entity must now require the service provider implement and maintain reasonable security procedures and practices that are reasonably designed to help protect the information from unauthorized access, use, modification, disclosure or destruction, as appropriate to the nature of the information disclosed to the service provider. A third-party service provider is defined as an entity that has been contracted to maintain, store or process personal identifying information on behalf of a covered entity.

4. Security Breach Notification Requirements Enhanced

The new law significantly amends Colorado's statute governing notifications of a security breach, C.R.S. § 6-1-716. A "security breach" is defined, in relevant part, as the unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality or integrity of personal information maintained by a covered entity.

Under the new provisions, a covered entity has no more than 30 days to provide notice of a security breach. Notice must be made to affected Colorado residents in a very specific manner including notice by mail, telephone, electronically or by substitute notice, and must contain a myriad of information regarding the breach and options that are available to the affected person. If a breach is reasonably believed to have affected 500 Colorado residents or more, the entity also must provide notice of the breach to the Colorado attorney general.

And, unlike the previous law, the 30-day period begins to run when the covered entity becomes aware that a "security breach may have occurred." In the prior version of the law, the 30-day period did not begin to run until the covered entity became aware of a breach. This change is likely to increase the pressure on covered entities to timely respond to indicators and predictors of a security breach.

Sanctions

Employers who violate the law can face enforcement proceedings from the Colorado attorney general or the district attorneys of the state. These proceedings can result in civil penalties of up to $2,000 per

affected person, up to a maximum of $500,000 per incident. They also can be liable directly to affected persons who are harmed by the violation.

Steps for Employers to Take

The new data security requirements go into effect on Sept. 1, 2018, so employers who maintain personal identifying information on Colorado residents have little time to prepare to comply. Steps to take include:

- Develop and implement reasonable practices designed to protect personal identifying information from unauthorized access, use or disclosure (e.g., password-protection, encryption, etc.) that are commensurate with the sensitivity of the personal identifying information.
- Create a written policy regarding the destruction and disposal of paper and electronic documents containing personal identifying information.
- Review agreements with third-party service providers to ensure that service providers have reasonable procedures to protect the security of personal identifying information provided to them.
- If you have a security incident response plan, update it to reflect the changes in the law.
- If you do not have a security incident response plan, prepare one to ensure that you can meet the new law's notification requirements.

Dustin Berger is of counsel at Holland & Hart LLP.