BARNES & THORNBURG LLP

ALERTS

California's New Data Protection Laws Are Coming … But Colorado's Law Is Already Here

November 14, 2018 | Atlanta | Chicago | Columbus | Dallas | Delaware | Elkhart | Fort Wayne | Grand Rapids | Indianapolis | Los Angeles | Minneapolis | New York | San Diego | South Bend | Washington, D.C.

Much has been said about California's comprehensive data protection and privacy law that goes into effect in 2020. Recently, Colorado enacted one of the most rigorous data protection legislations in the United States. Colorado's House Bill 18-1128, titled "Protections for Consumer Data Privacy," requires "covered entities" to comply with new rules regarding handling of "personal information" (PI). In addition to enacting a set of new data security standards, Colorado amended its existing data breach notification regime and introduced more stringent security breach notification timeframes. The new law went into effect Sept. 1, 2018.

Does the Law Apply to You?

If you are a business that maintains, owns, or licenses computerized data that includes PI about Colorado residents, this new law applies to you.

Summary of How the Law May Affect You

If you are subject to the new Colorado data protection law, you must at least:

- Have written security and privacy documents with policies and procedures;
- Have a written policy on deletion/destruction of PI; and
- Provide notification within 30 days of a "security breach" affecting information of any Colorado residents;
    - if the breach affects more than 500 Colorado residents, notify the Colorado attorney general;
    - if more than 1,000 Colorado residents affected, notify credit reporting agencies

The Basic Requirements of Colorado's Data Privacy Law

Covered Entities: The law applies to businesses that maintain, own, or license computerized data that includes PI about Colorado residents. Such "covered entities" must also maintain "reasonable security procedures and practices" appropriate to the nature of the PI they hold, and the nature and size of the business and its operations. (Importantly, even though the Colorado law uses the term "covered entities" that is also used by HIPAA, the term in the Colorado law is much broader.) The statute does not define "reasonable security procedures."

RELATED PEOPLE

Todd G. Vare
Partner
Indianapolis, Chicago

P 317-231-7735
F 317-231-7433
todd.vare@btlaw.com

Jason A. Bernstein
Partner
Atlanta

P 404-264-4040
F 404-264-4033
jason.bernstein@btlaw.com

Scott N. Godes
Partner
Washington, D.C.

P 202-408-6928
F 202-289-1330
scott.godes@btlaw.com

RELATED PRACTICE AREAS

Data Security and Privacy

Security Breach: The term “security breach” is defined as “the unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a covered entity.”

Personal Information: The statute protects Colorado residents’ PI and further expands that definition as any one or more of the following three sets of information:

1. First name or initial with last name, combined with
    1. Social Security number
    2. driver’s license or Colorado identification card number
    3. student, military, or passport identification number
    4. medical information
    5. health insurance identification number or
    6. biometric data
2. A resident’s username or email address, in combination with a password or security questions and answers, that would permit access to an online account; or
3. A resident’s account, credit card, or debit card number, even if not exposed in combination with an individual’s name*

* The disclosure of financial account information, even without disclosure of the individual’s name, reflects a broader definition of PI than in most other state laws.

Third-Party Service Providers: Businesses that disclose PI to third-party service providers must ensure that these service providers also implement and maintain “reasonable security procedures and practices” that are a) appropriate to the nature of the PI disclosed and b) reasonably designed to help protect the PI from unauthorized access, use, modification, disclosure or destruction.

Written Policies: Businesses must also develop and maintain written policies for the destruction of PI if such PI is no longer needed. Thus, documents that contain any PI no longer needed must be shredded, erased, or otherwise modified to make the PI unreadable or indecipherable through any means.

Data Breach Notification

Under the statute, businesses must notify Colorado residents of any security breach regardless of the number of affected individuals. If a business reasonably believes that the security breach has affected 500 or more Colorado residents, it must also provide notice to the attorney general “in the most expedient time possible and without unreasonable delay, but not later than 30 days.” The “determination that a security breach occurred” means “the point in time at which there is sufficient evidence to conclude that a security breach has taken place.”

Businesses must also notify the three national credit reporting agencies (TransUnion, Equifax, and Experian) if they reasonably believe that the security breach has affected 1,000 or more Colorado residents.

The notice to affected Colorado residents must include:

1. the date, estimated date or date range of the security breach
2. a description of the PI that was acquired, or reasonably believed to

have been acquired
3. contact information where the individuals may inquire about the breach
4. toll-free numbers, addresses, and websites for consumer reporting agencies
5. the toll-free number, address and website address for the Federal Trade Commission (FTC) and
6. a statement that the individual can obtain information from these sources about fraud alerts and security freezes

If the security breach involves a username or email address combined with a password or security question and answer that would permit online access to an account, businesses must direct affected individuals to change their password and security questions and answers, or to take other steps appropriate to protect the individual's online account.

If the breach involves the log-in credentials of an email account provided by the business, the business must provide notice:

1. through a method other than that email address and
2. by clear and conspicuous notice delivered at the time the individual is connected to the online account from an IP address or online location the covered entity knows the individual customarily accesses the account

Non-Compliance

Although the statute does not provide for a private right of action, the attorney general may bring an action in law or equity against covered entities to ensure compliance with the statute or recover direct economic damages.

Action Items

Colorado's new data privacy legislation, which reflects a broader approach to data security and privacy requirements, applies to companies that conduct business in Colorado, have Colorado employees, or interact with Colorado residents. All such entities are required to maintain appropriate security and data protection policies and develop internal procedures to ensure compliance.

For more information, please contact the Barnes & Thornburg lawyer with whom you work, or contact one of the following members of our data security and privacy practice group: Todd Vare at todd.vare@btlaw.com or 317-231-7735; Jason Bernstein at jason.bernstein@btlaw.com or 404-264-4040; Scott Godes at scott.godes@btlaw.com or 202-408-6928; or Michael Baumert at mbaumert@btlaw.com or 312-214-4570.