

# DIGITAL MEDIA, TECHNOLOGY & PRIVACY

>>ALERT

## STATES UPDATE DATA BREACH NOTIFICATION LAWS AMIDST GDPR COMMOTION

While the buzz surrounding the EU General Data Protection Regulation (GDPR) in the last month has dominated companies' attention, several states have made updates to their data breach notification laws, the city of Chicago has a data protection ordinance pending, and California enacted the [California Consumer Privacy Act of 2018](#). Many of these updates are consistent with general legislative trends seen in data breach notification laws both here in the US and under the GDPR.

In Colorado, Governor Hickenlooper recently signed a house bill to take effect September 1, 2018.

The bill amends Colorado's data breach notification laws (the "CO Amendment") to include, among other things, the following updates:

- >> The definition of "personal information" includes a Colorado resident's first name or first initial and last name in combination with certain other categories of information. The list of categories has been expanded by the CO Amendment to include: student ID, medical information, health insurance information, and biometric data.
- >> Notification of data breaches to affected Colorado residents must be made within 30 days of discovery. Previously, Colorado required notification "without undue delay" with no specific time limit.
- >> For the first time, Colorado law requires that a covered entity that "maintains, owns, or licenses personal identifying information of

### THE BOTTOM LINE

It is clear that local and state lawmakers are making data privacy protection requirements a legislative priority. As lawmakers continue to amend or enact new data protection and data breach notification laws, it will be crucial that all affected organizations ensure their policies and procedures are keeping pace and are compliant with the current state of the law.

an individual residing in [Colorado] shall implement and maintain reasonable security procedures and practices that are appropriate to the nature of the personal identifying information and the nature and size of the business and its operations." The CO Amendment also requires that appropriate security measures flow down to service providers receiving personal identifying information.

- >> Covered entities must have a written disposal policy for the proper destruction and disposal of both paper and electronic records containing personal identifying information that are no longer needed.

Louisiana amended its Database Security Breach Notification Law, which will take effect August 1, 2018 (the "LA Amendment"). The LA Amendment made similar updates as the CO Amendment:

- >> The definition of "personal information" includes a Louisiana resident's first name or first initial and law name in combination with certain other categories of information. The list of categories has been expanded by the LA Amendment to include a state identification card number, passport number and biometric data used to authenticate an individual's identity.

## DIGITAL MEDIA, TECHNOLOGY &amp; PRIVACY

## &gt;&gt;ALERT

- >> Like the CO Amendment, the LA Amendment now requires entities that conduct business in Louisiana or own or license computerized personal information about Louisiana residents to maintain “reasonable security procedures and practices” to protect such information.
- >> The LA Amendment also has a data destruction requirement for personal information that is “no longer to be retained,” but does not require a written disposal policy, as the CO Amendment requires.
- >> Notification to affected Louisiana residents must be made within 60 days of discovery of a breach.

Oregon also amended its data breach notification law (the “OR Amendment”), which took effect June 2, 2018. Among other updates, the OR Amendment now requires the following:

- >> The definition of “personal information” includes an Oregon resident’s first name or first initial and last name in combination with

certain other categories of information. The list of categories has been expanded by the OR Amendment to include information that would permit access to an individual’s financial account.

- >> Notification must now be made within 45 days following discovery of the breach.
- >> The OR Amendment also prohibits credit reporting agencies from charging a fee to consumers for placing a temporary security freeze on their credit reports.

Several other states made recently strengthened their data protection efforts, including Virginia (updated its breach notification laws to cover a taxpayer’s identification number in combination with income tax withholdings), Iowa (introduced an information security law geared towards protecting minors’ personal information), and Nebraska (introduced an information security law requiring reasonable security procedures and safeguards for personal information).

## FOR MORE INFORMATION

Gary A. Kibel  
Partner  
212.468.4918  
gkibel@dglaw.com

Justin H. Lee  
Associate  
212.468.4894  
jlee@dglaw.com

Vivian Wang  
Associate  
212.468.4927  
vwang@dglaw.com

or the D&G attorney with whom you have regular contact.

---

Davis & Gilbert LLP  
212.468.4800  
1740 Broadway, New York, NY 10019  
[www.dglaw.com](http://www.dglaw.com)  
© 2018 Davis & Gilbert LLP