CAPINTECH

What All Nonprofits Should Know About the New Colorado Data Privacy Law

By Allison Ward, Partner

A new Colorado data privacy law takes effect on September 1, 2018. Even if your nonprofit organization doesn't operate in Colorado, the law applies if you collect or maintain the personal data of Colorado residents.

Here's an overview of Colorado House Bill 18-1128 (the "Data Privacy Act") and how it may affect your organization.

Does the New Colorado Data Privacy Law Apply to You?

The law applies to "covered entities." A covered entity is defined as a person who "maintains, owns, or licenses personal identifying information in the course of the person's business, vocation, or occupation." This excludes individuals acting as a third-party service provider.

Compliance with other regulations may override compliance with some parts of the Colorado regulation.

Protecting Personal Identifying Information

Under the new law, personal identifying information (PII) includes:

- Social Security numbers
- Passwords
- Passcodes
- Official state or government-issued driver's license or identification card numbers
- Government passport numbers
- Employer, student, or military identification numbers
- Financial transaction devices

Covered entities are required to:

- Protect the PII of Colorado residents by implementing and maintaining "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."
- Ensure third-party service providers (such as donor system vendors) implement and maintain reasonable security procedures.
- Develop a written policy for the destruction and proper disposal of paper or electronic documents containing PII when the documents are no longer needed.

Notifying Residents of a Security Breach

The law also includes regulations for notifying Colorado residents of a breach of their personal information. This is different from the personal identifying information (PII) that must be protected.

Personal information includes a Colorado resident's:

- First name or initial and last name combined with any one or more of the following data elements when they are not encrypted, redacted, or secured (but note further information about encryption below):
  - Social Security number
  - Student, military, or passport identification number
  - Driver's license or identification card number
  - Medical information
  - Health insurance identification number
  - Biometric data
- Username or email address in combination with a password or security questions and answers
- Account numbers or credit or debit card numbers in combination with any required security or access code or password

If you are a covered entity and become aware that a security breach affecting personal information about

Colorado residents may have occurred, you must take the following steps:

- Conduct a "prompt investigation" to determine if misuse of the information has occurred or is likely.
- If misuse has not occurred and is not likely, notification is not required. (But the vulnerability that led to the breach should be fixed quickly.)
- If misuse has occurred or is likely, you must notify the affected Colorado residents no more than 30 days after determining that a security breach occurred, unless law enforcement requests that notification be delayed. The law outlines what must be included in the notification.
- Disclose the breach of encrypted or otherwise secured personal information if the encryption key or other means of accessing the information may also have been acquired in the security breach.
- Include specific warnings in the notification if the security breach involved a resident's username or email address *and* passwords or answers to security questions.
- If more than 500 residents must be notified, you must also notify the Colorado Attorney General within the 30-day period.
- If more than 1,000 residents must be notified, you must also notify all national consumer reporting agencies.

If a third-party service provider that maintains personal information for your organization believes it may have had a security breach, it must notify you if misuse of the personal information has or is likely to occur. The law states that this notification must occur "in the most expedient time possible, and without unreasonable delay." Since that is rather vague, we recommend including notification timeframes in your vendor agreements.

Penalties for Noncompliance

The Colorado Attorney General may take these actions if a covered entity is not in compliance:

- Request a court order to enforce compliance or to recover direct economic damages, or both
- Sue the covered entity
- Prosecute any criminal violations

New California Data Privacy Law on the Horizon

Next up: California Assembly Bill No. 375 (the "California Consumer Privacy Act of 2018") goes into effect on January 1, 2020. Considered to be the toughest consumer data privacy law in the United States, it will give consumers the right to request that businesses and organizations disclose what personal information is being collected, why it's being collected, and who it's being shared with, among other provisions.

Consumers will also be able to request that their personal information be deleted, opt out of the sale of their information, and receive their data in a "readily usable format" that can be transferred to another entity.

Under the new California privacy law, "personal information" notably includes geolocation information, Internet browsing history, and biometric data, among many other data elements. And consumers will be able to sue over data breaches if entities fail to protect their data adequately.

Note that this is a high-level summary of the new California privacy law. This article provides additional information.

Next Steps

- The European Union's General Data Protection Regulation (GDPR), which went into effect on May 25, 2018, and the new Colorado and California data privacy laws apply to organizations that collect or maintain personal information of residents of those regions. **We recommend that all nonprofit organizations carefully consider their interactions with EU, Colorado, and California residents to determine if the new laws apply to them.** Seek qualified legal counsel if you believe they might.
- **Create an Incident Response Plan or review your existing plan and make any necessary updates.** This should include procedures for notifying appropriate parties of a breach. Contact us at cybersecurity@capincrouse.com to request a sample Incident Response Plan.
- **Implement annual procedures and vendor reviews** to meet the requirements to protect the PII of residents.
- **Consider a Cybersecurity Assessment**, which will:
  - Help document that your organization has implemented "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," as required under the Colorado law.
  - Include an evaluation of your third-party vendors' due diligence efforts.
- **Consider obtaining cybersecurity insurance, if you don't already have it, and review and update any existing policies as needed.** Insurance coverage can help with the costs of security breach investigation and notification.

With the heightened focus on consumer data privacy, additional laws and regulations are likely. Even if your organization doesn't have a compelling reason to adhere to these new standards, however, they should be considered a best practice.

Beyond the potential legal consequences, a data breach can have a significant negative impact on your organization's operations, finances, reputation, and trust. Complying with these standards can help your organization reduce the risk of a breach and act quickly to minimize the damage if one does occur.

Please contact us at cybersecurity@capincrouse.com with questions or to learn more about how CapinTech can assist your organization with assessing and strengthening your cybersecurity controls and taking steps to comply with the new laws.

Even if your nonprofit organization doesn't operate in Colorado, the law applies if you collect or maintain the personal data of Colorado residents.

About the Author

Allison Davis Ward, Partner
CapinTech
award@capincrouse.com
o 505.50.CAPIN ext. 2008

Throughout her time as an information systems auditor, manager, and partner, Allison has provided information security assessment and consulting services for nonprofit organizations, financial institutions, health facilities, educational institutions, and a variety of other organizations. She stays current on changing threats to design review procedures to aid clients in implementing appropriate controls to protect against evolving cybersecurity threats. Allison speaks on information security topics for various banking, state CPA, and non-profit societies.

About CapinTech

CapinTech, a CapinCrouse company, provides information security services, including cybersecurity assessments, consulting, and training services, to financial institutions, nonprofit organizations, medical entities, professional services firms, and other organizations. Each year the firm performs hundreds of assessment, consulting, and speaking engagements with a team of experienced professionals retaining numerous certifications, including CPA, CISSP, CISM, CISA, CITP, CGMA, and CTGA. Each engagement is tailored to fit the unique needs of the organization, and information and reports are presented in a clear, concise manner intended for an audience with varying information systems (IS) knowledge. More information is available at capintech.com.

About CapinCrouse

As a national full-service CPA and consulting firm devoted to serving nonprofit organizations, CapinCrouse provides professional solutions to organizations whose outcomes are measured in lives changed. For over 50 years, the firm has served domestic and international outreach organizations, universities and seminaries, foundations, media ministries, rescue missions, relief and development organizations, churches and denominations, and many others by providing support in the key areas of financial integrity and security. With a network of offices across the nation, CapinCrouse has the resources of a large firm and the personal touch of a local firm. Learn more at capincrouse.com.

CapinCrouse is an independent member of the BDO Alliance USA.