Akin®

Colorado AG Issues Guidance on Data Security Best Practices

Apr 5, 2022

Reading Time : **3 min**

By: Natasha G. Kohne

The guidance advises entities to adopt the following nine practices:

1. Inventory types of data collected and establish systems to store and manage data.

Entities should take stock of all data that they collect and store, as well as the source and purpose of collection. From there, entities should develop written policies for data retention and destruction, along with limits on how long personal data will be retained.[2]

2. Develop a written information security policy.

Data minimization, access control, password management and encryption are crucial components of an information security policy, and entities should also consider any industry-specific rules applicable to the type of information being collected.[3]

3. Adopt a written data incident response plan.

A data incident response plan lays out the steps an entity will take if it becomes subject to a data incident, such as a data breach or cyberattack. The AG advises that incident response plans should be available in paper form in case a cyberattack jeopardizes computer access.[4]

4. Manage vendors' security.

Protecting data requires managing risks presented by other parties with access to an entity's systems, including third-party vendors. Once in effect, the CPA will require

entities to secure certain contractual obligations regarding data security from vendors processing personal information.[5]

5. Train employees to prevent and respond to cybersecurity incidents.

Similarly, entities should train their own employees on how to protect against phishing attacks by preparing them to identify and flag suspicious emails and network activity.[6]

6. Follow the Department of Law's ransomware guidance.

The Colorado Department of Law has separately issued guidance to entities facing increased threats of ransomware attacks. Among other things, entities are encouraged to quickly patch systems and make systems updates, test incident response plans and keep backups of system data. In the event of a ransomware attack, having accessible backups will ensure an entity can still operate even if its system has been rendered inaccessible due to encryption.[7]

7. Notify affected individuals and the Colorado AG of a breach, as required under law.

If an entity finds its network has been accessed by an unauthorized user, it should first conduct an investigation. If the entity concludes that personal information has been or is likely to have been misused, it has 30 days to notify affected Colorado residents, and must also notify the Colorado AG if 500 or more Coloradans are affected.[8]

8. Protect individuals affected by a data breach from identity theft and harm.

This may include compensating victims of a breach or undertaking other remedial measures, such as providing victims with access to free credit report monitoring.[9]

9. Review and update security policies regularly.

Data collection and data storage practices may need to be updated to respond to the constantly changing risks to personal information. Policies on data retention, data security and incident response should be reviewed regularly with this in mind.[10]

More and more State Attorneys General are issuing cybersecurity guidance, including the New York Attorney General's recently issued report on credential stuffing attack patterns and

how to defend against them. These guidelines further underscore the importance of regularly implementing, testing and updating data protection and cybersecurity practices.

Please contact a member of Akin Gump's cybersecurity, privacy and data protection team if you have any questions about this guidance or any of the outlined data security practices.

---

[1] C.R.S. §§ 6-1- 713.5, 716; "the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk and establish a clear allocation of the responsibilities between them to implement the measures." §§ 6-1-1305(4), (5).

[2] CO. Off. of the Attn'y Gen., *Data Security Best Practices* (February 14, 2022), available at https://coag.gov/app/uploads/2022/01/Data-Security-Best-Practices.pdf.

[3] *Id*. at 3.

[4] *Id*.

[5] *Id*. at 4.

[6] *Id*.

[7] *Id*. at 5.

[8] *Id*.

[9] *Id*. at 6.

[10] *Id*.

Categories

Consumer Privacy | State Privacy Policy | Cybersecurity & Information Security

© 2025 Akin Gump Strauss Hauer & Feld LLP. All rights reserved. Attorney advertising. This document is distributed for informational use only; it does not constitute legal advice and should not be used as such. Prior results do not guarantee a similar outcome. Akin is the practicing name of Akin Gump LLP, a New York limited liability partnership authorized and regulated by the Solicitors Regulation Authority under number 267321. A list of the partners is available for inspection at Eighth Floor, Ten Bishops Square, London E1 6EG. For more information about Akin Gump LLP, Akin Gump Strauss Hauer & Feld LLP and other associated entities under which the Akin Gump network operates worldwide, please see our Legal Notices page.