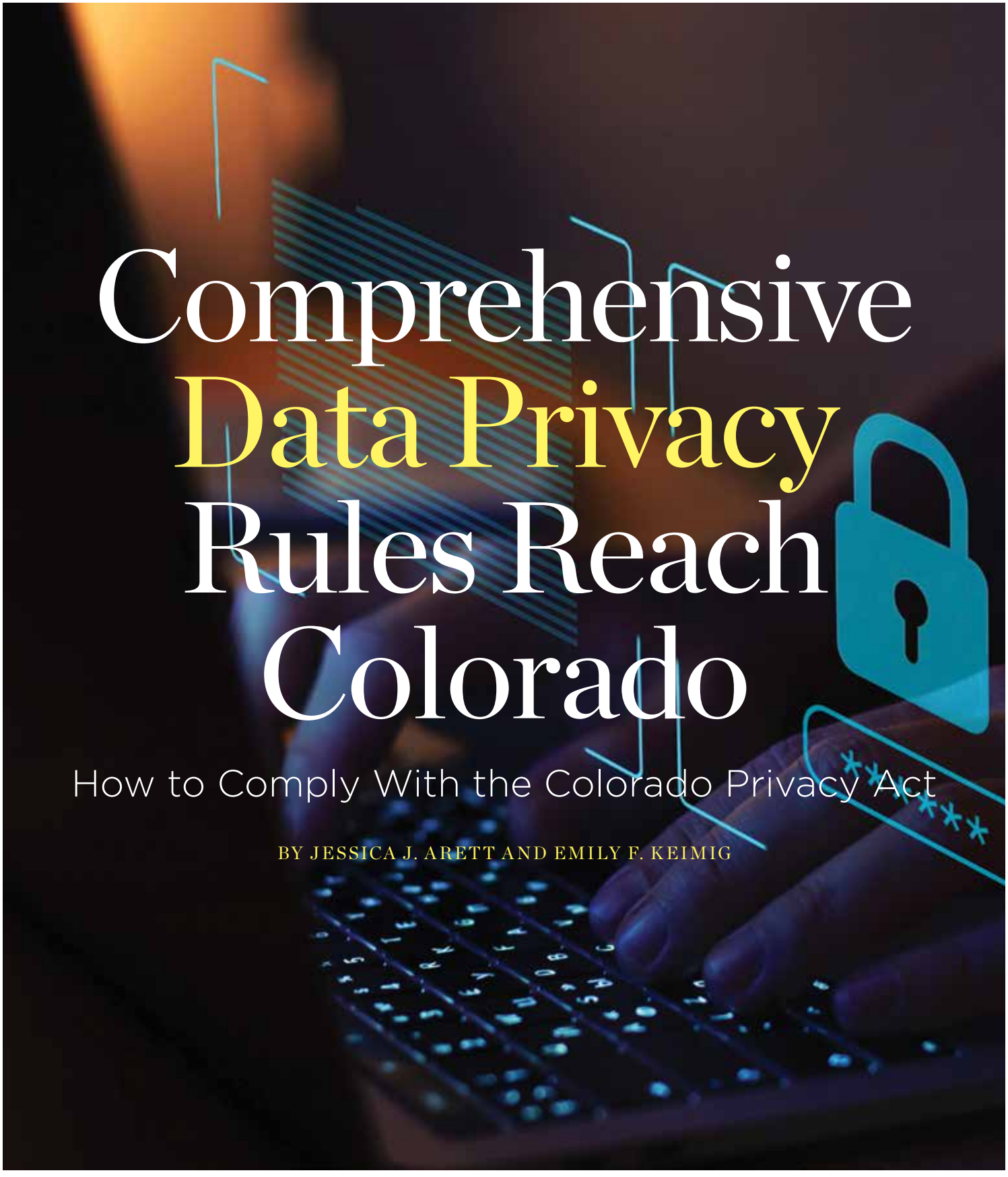

Comprehensive Data Privacy Rules Reach Colorado

How to Comply With the Colorado Privacy Act

BY JESSICA J. ARETT AND EMILY F. KEIMIG

This article discusses the provisions of the Colorado Privacy Act, a new law that imposes stricter requirements for protecting consumer data.

The last few years have seen a sea change in the way governments around the world address issues related to citizen and consumer privacy, and this year Colorado officially added to the tsunami. On July 1, 2023, the Colorado Privacy Act (the Act) came online, joining California,[1] Connecticut,[2] and Virginia[3] in this new frontier (with other states joining soon).[4]

Although the Colorado Attorney General's Office finalized the rules for the Act (rules) on March 15, 2023, many questions remain for companies seeking to implement compliance programs. This article provides an overview of the requirements of the Act and rules and offers practical tips for companies as they attempt to comply with the law.

General Framework of the Act

Though there are some key differences, Colorado's law is largely modeled from two similar laws—the California Privacy Rights Act (CPRA) and the European Union's General Data Protection Regulation (GDPR). The Act and its accompanying rules have certain distinct components that companies and nonprofit organizations interacting with Colorado consumers should consider when creating their privacy programs and policies.

Brief History of Recent Data Privacy Laws

In 2016, the European Union enacted the GDPR, which shifted the paradigm for thinking about data privacy.[5] Before the GDPR, most general privacy laws relied on a disclosure model: as long as companies disclosed to consumers how they intended to use their data, consumers had no choice but to either not engage with that company or accept that company's representation that it would use the consumers' data as disclosed. The GDPR changed this framework, requiring companies not just to disclose how they are using their data but also to have a legal basis for any given use. The GDPR also provided consumers with new rights, including the now-famous "right to be forgotten." Essentially, the GDPR shifted consumer data from a resource that companies had total control over to a resource that companies jointly control with the consumers who provide the data.

> "Importantly, and in contrast to the CPRA and the GDPR, the Act explicitly exempts from protections individuals acting 'in a commercial or employment context,' meaning that employment and business-to-business data is not subject to the Act."

The changed framework has been an attractive model for US lawmakers, because when state legislatures have considered comprehensive privacy laws, multinational companies have advocated for frameworks similar to the GDPR to simplify compliance. As a result, when California became the first state in the nation to pass a comprehensive privacy law, it borrowed much of its framework from the GDPR. Since then, the states that have enacted comprehensive data privacy laws, including Colorado, have done the same.[6]

What Data Is Protected?

The Act defines personal data as information that is linked or reasonably linkable to an identified or identifiable individual. The protections apply to data of "consumers," defined as Colorado residents "acting only in an individual or household context."[7] Importantly, and in contrast to the CPRA and the GDPR, the Act explicitly exempts from protections individuals acting "in a commercial or employment context," meaning that employment and business-to-business data is not subject to the Act.[8] This comes as a huge relief to employers in particular, as protections for employee data are typically covered by other, potentially conflicting, laws.

Who Must Comply?

Unlike the CPRA and the GDPR, Colorado's law specifically targets entities that process large amounts of personal consumer data. The Act uses many definitions found in the GDPR, including "controller" for entities that determine the purpose for and means of processing data

(defined as collecting, using, selling, storing, disclosing, analyzing, deleting, or modifying) and "processor" for entities like vendors that process data on behalf of a controller.[9] The Act applies to any legal entity (including a nonprofit entity) that conducts business in Colorado or provides products or services in Colorado that are "intentionally targeted" to residents of Colorado *and* (1) annually controls or processes personal data of at least 100,000 Colorado residents or (2) derives revenue (or receives discounts) from selling personal data *and* processes or controls the personal data of 25,000 or more Colorado residents.[10] Thus, the Act creates an incentive for companies to avoid selling or obtaining some economic benefit from selling personal data.

The Act exempts certain entities that are required to comply with other data privacy laws (such as financial institutions covered by the Gramm-Leach-Bliley Act). Furthermore, certain types of data are not subject to the Act (e.g., data that is already protected by HIPAA).[11]

Consumer Rights

One of the Act's primary goals is to provide consumers with more control over their data held by entities subject to the Act. As a result, the Act grants consumers new rights, including the rights to access, correct, and in some cases delete data held by the entity about them; the right to obtain a copy of their personal data in a portable format; and the right to opt out of certain uses of their data.[12] Specifically, the opt-out gives consumers the right to opt out of (1) the processing of their personal data for purposes of targeted advertising, (2) the sale of their personal data, and (3) the use of their data for "profiling" when the profiling is done as part of a decision that has legal or similarly significant effects on the consumer.[13]

Starting on July 1, 2024, the Act will also require entities to honor user-selected universal opt-outs for targeted advertising and sales.[14] These universal opt-out mechanisms will likely take the form of a browser add-on. However, to date, there is no consensus about how a universal opt-out mechanism will work. And given that Colorado is the first state in the country to include this sort of provision in its Act, it is likely that implementation of this provision may prove uneven at first as regulators come to a consensus on the appropriate mechanism.

"Finally, the Act requires an entity to obtain a consumer's opt-in consent before processing sensitive data, which includes children's data, certain genetic or biometric data, and personal data revealing racial or ethnic origin, religious beliefs, a mental or physical health condition, sex life or sexual orientation, or citizen status."

Finally, the Act requires an entity to obtain a consumer's opt-in consent before processing sensitive data, which includes children's data, certain genetic or biometric data, and personal data revealing racial or ethnic origin, religious beliefs, a mental or physical health condition, sex life or sexual orientation, or citizen status.[15] The rules from the attorney general's office make clear that such consent requires a specific, affirmative action or statement, meaning that a statement that use of the website constitutes consent or acceptance of general terms and conditions will likely not be sufficient.[16] The design of the consent also cannot be "weighted" to consenting (such as having the consent button bolded or highlighted).[17] Additionally, the rules require an entity to obtain a "refreshed consent" if the consumer has not engaged with the entity for more than 24 months.[18]

The Act provides for exceptions to a consumer's rights in certain situations. If an entity determines that it is not required to act in response to particular requests, it must notify the consumer of the reasons for not taking the action and provide the consumer with instructions to appeal the decision. Upon receiving an appeal, the entity has 45 days to inform the consumer of its decision. That communication must include an explanation for the decision and inform the consumer of their ability to contact the attorney general's office if they have concerns about the results of their appeal.[19]

Many of these rights create conflicting interests between transparency and an entity's desire to maintain confidentiality of certain of its processes and trade secrets. The rules attempt to address this tension. For example, the rules state that if disclosure of personal data in a portable format would disclose trade secrets, the entity only needs to provide as much data as possible without disclosing the trade secret.[20]

Entity Obligations

The Act borrows heavily from both the CPRA and the GDPR in structuring entity obligations for responding to requests from consumers to exercise their rights under the Act. Entities must respond to all consumer requests within 45 days and provide consumers the right to appeal any decision by the entity not to take the action requested. The Act requires that entities disclose to consumers how they are using their personal data, and the rules require that those disclosures be understandable and accessible to the entity's target audience.[21] Under the Act, entities must also limit their collection and use of personal data to that which is reasonably

necessary and compatible with the purpose disclosed to consumers and obtain consent from consumers before processing personal data for a purpose not originally disclosed.[22] The Act also mandates that entities maintain reasonable measures to keep personal data confidential.[23] This mandate requires entities to conduct periodic data protection assessments to evaluate risks associated with certain higher-risk processing activities and to document the assessments and make them available to the attorney general's office upon request.[24] The rules provide a detailed list of at least 13 items required to be included in each assessment.[25]

Finally, if an entity uses a third party to process some of the personal data, the Act requires that the entity and third party contractually define their relationship to ensure that the third party is also complying with the obligations of the entity. The contract must provide for audits of the third party's actions to ensure contract compliance.[26]

Enforcement

The Act is solely enforced by the Colorado Attorney General and state district attorneys—it does not provide a private right of action to consumers.[27] Acknowledging that the Act is imposing many new and, as yet, untested obligations, the Act requires the government to provide the entity with a 60-day cure period for any alleged violation. That cure period requirement expires in 2025, under the assumption that, by then, entities should have had time to get up to speed on compliance.[28]

The ramifications for violating the Act are significant, with each violation (measured per consumer and per transaction) punishable by civil penalties up to $20,000.[29]

Because comprehensive privacy laws do represent a significant paradigm shift in how companies treat consumer data, Colorado is not unique in reserving enforcement authority to the government. California does permit a private right of action for consumers who have certain types of data exposed in a data breach, but otherwise also leaves enforcement of its statute up to the state government.[30] The other states that have implemented similar laws have followed Colorado and have chosen to reserve all enforcement authority to the state. However, creative plaintiffs' lawyers may still find ways to bring private lawsuits for violations under other legal theories, including unfair trade practices acts and other consumer protection laws.

Achieving Compliance

The Act became effective on July 1, 2023, but has a one-year lookback period and applies to data collected since July 1, 2022. Affected entities should ensure they have a compliance program in place that takes into account the points below.

Know What Data You Have and Where It Resides

The first step in preparing a compliance program is to understand what (and how much) consumer data your entity maintains. This will require determining the various sources of data collected by all departments (directly from consumers, data pulled from cookies and other automated means, and data obtained from third parties); understanding the purpose for each type of data owned; and knowing where and how it is maintained.

Determine the Necessity of Each Data Category

Although we do not yet know which aspects of the law government actors will focus on, if the efforts of government actors in Europe are any indication, one area will likely be on whether entities are complying with their data minimization obligations. Therefore, to reduce enforcement risk, entities should assess whether each type of data that is collected is essential to accomplish the goals of the organization and discuss limiting the collection of data that may not be crucial. Additionally, each entity should review its preservation policies to ensure that data is not held for longer than necessary.

Assess and Adjust Security Measures

Once an entity determines what data it needs, the next step is to ensure that the data is protected appropriately. The level of protection necessary will depend on the sensitivity of the data. To the extent possible, entities should implement a privacy-by-design approach, building as many security features as possible into the system rather than requiring implementation by individual employees. Common practices include encryption, pseudonymization, cabining data so that only employees who need to use the data can access it, implementing technical safeguards such as firewalls and antivirus protections, and training employees regularly on the importance of data security. An entity should also have an incident response plan in place to respond if a data breach does occur.

Document Data Impact Assessments

Document all efforts to assess the data you collect, including how that data is protected. You should include your reasons for making certain decisions regarding what data is necessary to collect and what security measures to put in place. This will not only provide you with the documentation necessary if the attorney general asks for your last data impact assessment, but will also assist in ensuring accountability for all teammates in following the decisions made regarding the handling of data.

Update Your Privacy Policy

The Act requires privacy policies to clearly inform consumers about the data they collect, including how the data is used and the consumer's rights under the Act. Essentially, the adage "say what you do and do what you say" is more applicable than ever. Unfortunately, the Act's mandate that an entity be specific and comprehensive with the information it discloses conflicts with the rules that the policy be understandable and accessible to the entity's target audiences (i.e., avoid technical and legal jargon). This will be especially complicated for entities that also need to comply with other state and international privacy laws because in such instances the disclosure will need to explain how the consumer's geographic location impacts their legal rights.

Update Vendor Agreements

The Act requires entities to include specific provisions in agreements with third-party vendors who will have access to consumer data. These provisions are similar to those in the GDPR and include:

1. processing instructions to which the vendor is bound;

2. a list of the types of personal data subject to processing by the vendor and the duration of that processing;
3. a requirement that data will be deleted or returned to the entity when the relationship with the vendor concludes;
4. a statement that the vendor will make necessary information available to the entity for audits; and
5. a statement that the vendor must adhere to the entity's instructions and flow down contractual obligations to sub-processors.[31]

Any entity subject to the Act must ensure that its vendor agreements include these provisions. Entities should also conduct periodic audits on their vendors and document the results of those audits.

Develop a Process for Responding to Consumer Requests and Obtaining Consent

In order to respond to requests from consumers for their data, many entities will need to implement an entirely new set of processes. Given the Act's 45-day timeframe, an entity will need to have a process in place that allows it to quickly and efficiently locate all of the data it (or any of its third-party vendors) maintains on any given consumer, provide that data to the consumer, and be capable of deleting or correcting the data if requested. The rules require entities to provide two methods for a consumer to submit a data rights request. Before data can be handed over in response to a request, the entity must employ a process to confirm the consumer's identity using methods that are commercially reasonable based on the level of sensitivity of the data. Additionally, to prepare for the universal opt-out mechanism provision that becomes effective in July 2024, the entity must make sure that it can respond to requests from consumers who exercise their rights through such a mechanism.

Train Employees on the Privacy Program

Unless employees understand the processes in place for ensuring compliance and the importance of following those processes, a data privacy policy is nothing more than words on paper (or a screen). An entity should regularly train employees on the new processes put in place to comply with the Act (and document those training programs).

Conclusion

The evolution of data privacy law has been drastic over the last few years. While many of the Act's provisions will be familiar to companies subject to GDPR and the CPRA, the Act contains novel provisions that all companies subject to the Act will need to comply with. Moreover, the Act's application to nonprofit entities means that those organizations will now need to implement privacy protocols that they may have previously avoided. And given the direction and proliferation of laws in this area, all entities, including those not subject to the Act, should assess the role of data in entity operations and identify areas that may conflict with the data transparency and minimization principles that all of these laws are grounded on. CL


Jessica J. Arett is a member in Sherman & Howard L.L.C.'s litigation group and data security and privacy group—jarett@shermanhoward.com. **Emily F. Keimig** is a member in Sherman & Howard L.L.C.'s employment group and litigation group and heads the firm's data security and privacy group—ekeimig@shermanhoward.com.

Coordinating Editor: Todd R. Seelman, todd.seelman@lewisbrisbois.com

NOTES

1. Cal. Civ. Code §§ 1798.100 to 1798.199.100.
2. 2022 Conn. Acts 22-15 (Reg. Sess.).
3. Va. Code Ann. § 59.1-575.
4. Indiana, Iowa, Montana, Oregon, Tennessee, Texas, and Utah have all passed similar laws that will go into effect over the next few years.
5. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, 2016 O.J. (L 119).
6. *See supra* notes 1–4. *See also* "Prepared Remarks: Attorney General Phil Weiser on The Way Forward on Data Privacy (May 4, 2023)" (discussing background on the Act), https://coag.gov/blog-post/prepared-remarks-attorney-general-phil-weiser-on-the-way-forward-on-data-privacy-may-4-2023.
7. CRS § 6-1-1303(6).
8. *Id.*
9. CRS § 6-1-1303(7), (19).
10. CRS § 6-1-1304(1) (emphasis added).
11. CRS § 6-1-1304(2).
12. CRS § 6-1-1306(a)–(e).
13. CRS § 6-1-1306(a).
14. *Id.*
15. CRS §§ 6-1-1308(7) and -1303(24).
16. 4 CCR 904-3, Rule 7.03.
17. 4 CCR 904-3, Rule 7.09.
18. 4 CCR 904-3, Rule 7.08.
19. CRS § 6-1-1306(2).
20. 4 CCR 904-3, Rule 4.07(B).
21. CRS § 6-1-1308(1); 4 CCR 904-3, Rule 3.02(A)(1).
22. CRS § 6-1-1308(2)–(4).
23. CRS § 6-1-1308(5).
24. CRS § 6-1-1309.
25. 4 CCR 904-3, Rule 8.04.
26. CRS § 6-1-1305(5).
27. CRS § 6-1-1311.
28. CRS § 6-1-1311(1)(d).
29. CRS § 6-1-1311(1)(c).
30. Cal. Civil Code § 1798.150(a)(1).
31. CRS § 6-1-1305(5).