The Rising Tide of Consumer Data Privacy Legislation

Mark Sadler, JD, CIPP/US, RPLU, CPLP

Overview / Introduction

This was a watershed year for consumer data privacy legislation. At the start of the year five states had enacted consumer data privacy statutes; by the end of 2023, the count was up to thirteen states.[1] In addition, three states had enacted legislation directed at protecting the privacy of consumer health decisions and health data. The trend is expected to continue into 2024 and beyond.[2]

While there are numerous factors driving the trend, one reason may be a perceived inadequacy with the U.S. sectoral approach to privacy and changing public opinions regarding data security and privacy. Further, some have cited the lack of an omnibus federal privacy statute as a reason for the state level interest in consumer privacy legislation; while there have been efforts to introduce and pass an omnibus federal privacy law, the *American Data Privacy and Protection Act* has been unable to gain sufficient support to date in Congress for passage.[3]

A study by the Pew Research Center concluded that "[a] majority of Americans (64%) have personally experienced a major data breach, and relatively large shares of the public lack trust in key institutions – especially the federal government and social media sites – to protect their

[1] *See* Luke Schaetzel, *Privacy Floodgates Open: 13 U.S. States Now Have Omnibus Data Protection Laws on the Books,* Benesch Data Meets World (October 2, 2023), *available at*: https://www.beneschlaw.com/resources/privacy-floodgates-open-13-us-state-data-protection-bring-about-major-changes.html.

[2] *See*, *Gartner Identifies Top Five Trends in Privacy Through 2024*, Gartner, Inc. (May 31, 2022), *available at*: https://www.gartner.com/en/newsroom/press-releases/2022-05-31-gartner-identifies-top-five-trends-in-privacy-through-2024. (According to Nader Henein, a Vice President and Analyst at Gertner, "By year-end 2024, Gartner predicts that 75% of the world's population will have its personal data covered under modern privacy regulations. This regulatory evolution has been the dominant catalyst for the operationalization of privacy.")

[3] *American Data Privacy and Protection Act Topic Page*, International Association of Privacy Professionals (2023), *available at*: https://iapp.org/resources/topics/adppa/#:~:text=As%20summarized%20on%20the%20U.S.,bill%20can%20be%20found%20here. (According to the International Association of Privacy Professionals, "[t]he proposed ADPPA, and its legislative path are the closest U.S. Congress has ever been to passing comprehensive federal privacy legislation. As summarized on the U.S. Library of Congress, 'This bill establishes requirements for how companies, including nonprofits and common carriers, handle personal data, which includes information that identifies or is reasonably linkable to an individual.'")

personal information."[4] In addition, reports of high profile cyber events such as the Equifax breach, Solarwinds, Blackbaud, Kaseya and the MOVEit event have raised the issue of data security and privacy in the perception of the public. These trends have provided additional support for a legislative response.

In May of 2018, the European Union General Data Protection Regulation became effective and in June of 2018, the first state consumer data privacy law, the California Consumer Privacy Act, was signed into law. Subsequent enactment of consumer data privacy legislation has ushered in a trend that some believe may eventually encompass most of the states in the United States. As of the date of this writing, consumer data privacy statues have been enacted in California, Connecticut, Colorado, Virginia, Utah, Iowa, Indiana, Florida, Montana, Tennessee, Texas, Delaware, and Oregon.

This paper will briefly discuss the legislative rationale for these laws as well as discuss some of the common provisions seen thus far in these consumer data privacy statutes. I will also discuss a recent trend in the passage of state privacy laws directed to health data and privacy. I will conclude with some recommendations for entities in navigating this new legal environment.

The New Consumer Data Privacy Legislation

Historically, a primary privacy concern for business, nonprofits and public entities in the United States has been compliance with statutes that specify data protection standards and notification requirements in the event of a data breach. All fifty states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have enacted data breach reporting laws requiring entities such as private businesses, governmental entities, and non-profits to notify individuals and regulators in the event of a security breach involving personally identifiable information.[5]

[4] Kenneth Olmstead and Aaron Smith, *Americans and Cybersecurity*, The Pew Research Center (January 26, 2017), *available at*: https://www.pewresearch.org/internet/2017/01/26/americans-and-cybersecurity/.

[5] The information covered as personally identifiable information or PII by these statutes includes a data subject's first and last name in combination with a data element specified by the statute, such as a social security number, driver's license number of financial account number. One of the rationales for these laws is prevention or mitigation of the risk of identity theft.

Under the sectoral regulatory structure in the United States, data privacy laws have generally been categorized by *industry* (e.g., Health Insurance Portability and Accountability Act and the Gramm–Leach–Bliley Act), by the *type of data impacted* (e.g., Video Privacy Protection Act) and the *target of the services* (e.g., Children's Online Privacy Protection Act of 1998).

In recent years some experts have opined that the existing laws in place to protect data privacy are inadequate.[6] Following enactment and implementation of the General Data Protection Regulation in the European Union, several states considered consumer data privacy legislation that greatly expands the rights of data subjects, beyond the protection provided by sectoral federal and state laws and data protection statutes. One rationale for these efforts was the lack of an overall omnibus data privacy and protection law. For example, as stated in the legislative bill analysis for the Texas Data Privacy and Security Act, "[i]n the absence of robust federal regulations regarding the collection and use of consumer data, a movement has begun at the state level with various state legislatures looking to set their own standards."[7] Others have opined that the comprehensive or omnibus consumer data privacy trend is, at least in part, a result of state lawmakers satisfying long-term privacy ambitions and lobbying activity.[8]

According to the national conference of State Legislatures consumer data privacy legislation was considered in sixty (60) bills in at least twenty five (25) legislatures during 2023.[9] The rationale for these new laws varies by jurisdiction. For example, in Virginia, the objectives included providing a framework for controlling and processing personal data; outlining responsibilities and privacy protection standards for data controllers and processors; and, granting consumers a right

[6] Thorin Klosowski, *The State of Consumer Data Privacy Laws in the U.S. (and Why it Matters)*, New York Times Wire Cutter (September 6, 2021), *available at*: https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/. (As noted in a New York Times blog, "[c]urrently, privacy laws are a cluttered mess of different sectoral rules. 'Historically, in the US we have a bunch of disparate federal [and state] laws,' said Amie Stepanovich, executive director at the Silicon Flatirons Center at Colorado Law. '[These] either look at specific types of data, like credit data or health information,' Stepanovich said, 'or look at specific populations like children, and regulate within those realms.'")

[7] Bill Analysis H.B. 4, Texas Senate Research Center (May 2, 2023), *available at*: https://capitol.texas.gov/tlodocs/88R/analysis/html/HB00004H.htm.

[8] *See*, Joseph Duball, *State Privacy Dispatch: Why the Floodgates Opened*, International Association of Privacy Professionals (May 15, 2023), *available at*: https://iapp.org/news/a/state-privacy-dispatch-the-floodgates-are-open/.

[9] Heather Morton, *2023 Consumer Data Privacy Legislation,* National Council of State Legislatures (September 28, 2025), *available at*: https://www.ncsl.org/technology-and-communication/2023-consumer-data-privacy-legislation.

to access, correct, delete, obtain a copy of personal data, as well as a right to opt out of the processing of personal data for purposes of advertising.[10]

In its *2022 Privacy Law Update*, Gardner Law outlines several other common threads present in recent state consumer data privacy legislation, including: (i) *transparency* (disclosure of what data is being collected and how it is used); (ii) *lawful and legal basis for collection* (identification of the legal basis for collecting data); (iii) *limiting data collection to only the amount and type of data necessary*; (iv) *accountability* (considering whether data will be transferred to third parties or across international borders and specifying the security and privacy protections in place); (v) *limited retention* (having custody of data only as long as is reasonably necessary to accomplish the purpose for which is was collected); *individual rights* (making data available to the data subject including rights such as the right to inspect, delete, restrict and rectify data as well as control data portability); and (vi) *data security* (maintaining the confidentiality, integrity and availability of personal information maintained by a data controller).[11]

Comparison of Key Privacy Provisions

The consumer data privacy statutes passed to date contain several common elements that create a set of consumer rights, generally enforceable by the Attorney General of the applicable state. There is understandable interest on the part of organizations subject to these new laws, especially considering compliance by organizations that operate in multiple jurisdictions that may be subject to these new laws. To address this concern, a systematic analysis of the common elements of the new laws may be helpful, including consideration of the following categories:

Applicability Thresholds:

Most consumer data privacy laws apply to businesses operating or doing business in the jurisdiction in question. There are triggers that must be met for a state's data protection law to apply, including: (i) a specific amount of annual gross revenue that must exceed a threshold; (ii) collection of personal information from consumers that must meet a threshold; and (iii) collection and sale of a consumer personal information. Some states require that the revenue threshold be

[10] S.B. 1392, *Consumer Data Protection Act; personal data rights of consumer, etc.*, 1st Spec. Sess. (Va. 2021), *available at*: https://lis.virginia.gov/cgi-bin/legp604.exe?212+sum+SB1392.
[11] *See*, *2022 Privacy Update*, Gardner Law (September 6, 2022), *available at*: https://www.jdsupra.com/legalnews/2022-privacy-update-2147723/.

met before additional thresholds are considered. For example, in Montana the threshold is (ii) 50,000 consumers' information processed or (iii) 25,000 consumers information processed and 25% + of gross, worldwide revenue from selling personal information.[12] In California the revenue threshold is gross annual revenues above $25 million or 100,000 consumers information bought, sold, or shared, or 50%+ of annual revenue from selling personal information.

However, even if the thresholds are met, some states exempt regulated entities such as healthcare entities, financial services firms, nonprofits, or native tribes.

Exclusion of Applicants and Former Employees:

The states have generally not applied their consumer data privacy laws to employees, applicants, or former employees in their definition of protected persons. For example, in Virginia, the Act applies to "a natural person who is a resident of the Commonwealth acting only in an individual or household context." There is an exception for "a natural person acting in a commercial or employment context."[13] A notable exception is the California Consumer Protection Act, personal information is defined in a manner that may include an employee information such as contact information, insurance and benefits elections, emergency contacts, dependents, compensation history, etc.[14]

***Rights of Data Subjects*:**

Consistent with the purpose for which the consumer data privacy laws were enacted, the laws contain an expanded set of rights for consumers regarding protection and management of their personal data in the custody of entities covered by the laws. For example, there are rights to delete data or be forgotten; a right to correct inaccurate data and a right to receive confirmation of the

---

[12] *See*, Luke Schaetzel, *Privacy Floodgates Open: 13 U.S. States Now Have Omnibus Data Protection Laws on the Books,* Benesch, Friedlander, Coplan & Aronoff LLP (October 2, 2023) *available at*: https://www.beneschlaw.com/resources/privacy-floodgates-open-13-us-states-now-have-omnibus-data-protection-laws-on-the-books.html.

[13] Sarah Rippy, *Virginia Passes the Consumer Data Protection Act*, International Association of Privacy Professionals (March 3, 2021), *available at*: https://iapp.org/news/a/virginia-passes-the-consumer-data-protection-act/.

[14] *See*, Nate Garhart and Rebecca Stephens, *Employer Exemptions Under the CCPA*, Society for Humay Resource Management (January 20, 2023). *available at*: https://www.shrm.org/resourcesandtools/legal-and-compliance/state-and-local-updates/pages/employer-exemptions-under-the-ccpa.aspx#:~:text=Indeed%2C%20under%20the%20CCPA%2C%20personal,grants%2C%20compensation%20history%2C%20and%20other

individual's personal data held by regulated entities. In addition, in line with the focus on protecting individuals from unauthorized sale of their data, the laws typically contain a right to restrict the sale of their personal data or sharing of their personal data for behavioral advertising.[15]

***Private Enforcement / Private Right of Action*:**

A private right of action "allows a private plaintiff to bring an action based directly on a public statute, the Constitution, or a federal common law."[16] Consistent with other state privacy laws, most of the recently enacted consumer data privacy laws do not permit a private right of action, but rather, vest enforcement with governmental authorities. A notable departure is the California Consumer Protection Act,[17] that "gives individuals the right to seek statutory damages against a business in limited circumstances involving the [CCPA as amended] reasonable security obligation."[18] Under the law, "California residents have the right to bring a lawsuit under the [CCPA as amended] only in certain circumstances. Specifically, the consumer must demonstrate that "nonencrypted and nonredacted personal information . . . [was] subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information."[19]

***Cure Periods*:**

A cure provision allows an entity the opportunity to correct an alleged violation of a comprehensive liability statute prior to being subject to an enforcement action or penalties. These provisions provide an entity the opportunity to avoid enforcement or a claim by correcting an alleged deficiency. As explained by one commentator, "[t]he nondiscretionary right to cure and the discretionary opportunity to cure will both preclude the state from initiating formal enforcement actions for a statutorily sanctioned time-period after notice of the alleged violation is

---

[15] *See*, Dustin Berger, *Leaning Toward Commonality: State Enact New Comprehensive Consumer Data Privacy Laws*, Dorsey & Whitney*, LLP* (June 14, 2023), *available at*: https://www.dorseyhealthlaw.com/2019-2/.

[16] Caroline Bermeo Newcombe, *Implied Private Rights of Action: Definition, and Factors to Determine Whether a Private Action Will Be Implied from a Federal Statute*, 49 Loyola University Chicago Law Journal 120 (Fall 2017).

[17] Please note that the California Privacy Protection Act, or CCPA, was amended effective January 1, 2023, as a result of a ballot initiative that passed in November 2020. Therefore, I will use refer to this law as the "CCPA as amended" to refer to this legislation in this paper.

[18] Tara L Trifon and Lindsey E. Kress, *The Murky Waters of the CCPA's Private Right of Action: Real and Perceived Ambiguities Complicating Litigation,* Locke Lord, LLP (November 2000), *available at*: https://www.lockelord.com/newsandevents/publications/2020/11/the-murky-waters.

[19] *Id*.

received. Enforcement proceedings are prohibited if alleged violations are cured during a specific time. In addition to curing the alleged violative act or practice, parties that receive written notice of alleged violations must also provide evidence of voluntary efforts to implement new and more secure mechanisms and practices in the collection and use of consumer data and make regular reports to the state Attorney General's office."[20]

***Civil Penalties*:**

Each of the consumer data privacy statutes contains a monetary penalty for violation of the Act. The common per violation penalty amount is $7,500 - $15,000. Depending on the severity of the violation, the penalties can be substantial. For example, "[i]n August 2022, the California Attorney General reached a $1.2 million settlement with *Sephora*, the makeup and skincare retailer, finding that its sharing of consumer data with analytics and social media companies for discounted services or other non-cash compensation is a 'sale' under the [CCPA as amended] requiring a 'Do Not Sell my Personal Information' button on the company's website and other actions."[21]

***Additional Data Category – Sensitive Data*:**

Sensitive data is a legal category of personal information that requires special handling under the General Data Protection Regulation, the California Privacy Rights Act, and other consumer data protection statutes. As explained by Marsha Komnenic, an Information Security and Data Privacy Specialist, "[w]hile the legal definition of personal information changes under different privacy laws, it refers to any data that can directly or indirectly identify an individual or household. Sensitive information, however, can be used to determine things like a person's opinions, personal preferences, or additional susceptible details that could lead to fraud, identity theft, or other harm if the data is leaked, breached, or compromised in some way."[22]

---

[20] Micah Russel, *Comparing U.S. Comprehensive State Privacy Laws: Enforcement and Opportunity to Cure*, Network Advertising Initiative (August 14, 2023), *available at*: https://thenai.org/comparing-u-s-comprehensive-state-privacy-laws-enforcement-opportunity-to-cure/.

[21] Michael R. Cohen and Tedrick A. Housh III, *Are You Ready For 2023's New Data Privacy Laws?* Lathrop GPM (January 5, 2023), *available at*: https://www.lathropgpm.com/newsroom-alerts-72704.html.

[22] Marsha Komnenic, CIPP/E, CPT, FIP, *Personal vs. Sensitive Personal Information*, Termly, Inc. (February 3, 2023), *available at*: https://termly.io/resources/articles/sensitive-personal-information/.

Protection of sensitive data under the state consumer data privacy statutes began with the California Consumer Protection Act and is also reflected in the Colorado Privacy Act, the Virginia Consumer Data Protection Act, the Utah Consumer Privacy Act, and the and Connecticut Act Concerning Personal Data Privacy and Online Monitoring.[23] Under these laws, sensitive data is afforded additional protection,[24] and as recently explained by a leading privacy expert, "sensitive data goes beyond the definition of 'personal data' to include data relating to racial or ethnic origin, religious beliefs, mental of physical health diagnosis, sexual orientation or genetic and biometric data as recognizing the need for heightened protection requirements.[25] For example, "the Virginia Consumer Data Protection Act and the Colorado Privacy Act require[s] express consent and a data protection impact assessment to process sensitive data."[26]

Health Data Privacy Laws

In addition to new consumer data privacy laws, 2023 also saw the emergence of new privacy laws directed to protecting the privacy of consumer health decisions and health data. The first of these statutes was the *Washington My Health Data Act* which is intended to close the gap between health insurance industry practices and the current methods used by health care entities to collect, store and transfer data. According to some, the law is intended to "respond[] to the U.S. Supreme Court decision in Dobbs v. Jackson Women's Health Organization and protect[] Washingtonians' health privacy, especially for reproductive health care."[27] According to the Office of the Attorney General

---

[23] *See*, Prof. Daniel J. Solove, George Washington University Law School*, Data Is What Data Does: Regulating Based on Harm and Risk Instead of Sensitive Data*, 118 Nw. U. L. Rev. (forthcoming 2024), *available at*: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4322198.

[24] *Id*. at 6.

[25] *Id*. at 13. (Prof. Solove observes that "In the United States, all of the state consumer privacy laws passed thus far (California, Connecticut, Colorado, Virginia, and Utah) recognize the following categories of sensitive data: racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, genetic or biometric data. [In addition,] [m]any laws (except Utah and California) also recognize personal data collected from a known child as sensitive data. The laws all recognize citizenship or immigration status except California. The California Consumer Privacy Protection Act also recognizes the following types of data as sensitive: Social Security, driver's license, state identification card, or passport number, account log-in details, financial account, debit card, or credit card number; philosophical beliefs, trade union membership, contents of mail, email, and text messages, unless the business is the intended recipient of the communication. [However,] [u]nlike the GDPR, the U.S. state laws do not recognize political opinions as sensitive data. Additionally, most U.S. state laws (except for the CCPA AS AMENDED) fail to recognize philosophical beliefs as sensitive data like the GDPR.")

[26] *Id*. at 16.

[27] Amy Olivero and Anokhy Desai, *Washington's My Health, My Data Act,* International Association of Privacy Professionals (April 2023), *available at*: https://iapp.org/resources/article/washington-my-health-my-data-act-overview/.

for the State of Washington, "[t]he Act was developed to protect a consumer's sensitive health data from being collected and shared without that consumer's consent. Washington's concern for the urgent need to enhance privacy protections for health data is widely shared: 76% of Washingtonians express support for the My Health My Data Act." [28]

Generally, the Washington law applies to "all persons and businesses that conduct business in Washington (or provide services or products to Washington), and that collect, process, share, or sell consumer health data are impacted by the Act."[29] The Act defines a regulated entity as a "legal entity that (a) conducts business in Washington, or produces or provides products or services that are targeted to consumers in Washington and (b) alone or jointly with others, determines the purpose and means of collecting, processing, sharing, or selling of consumer health data. An entity that only stores data in Washington is not a regulated entity."[30] The law focuses on consent of the data subject and "requires one of two possible legal bases for processing health-related data: consent or necessity. Either consent or necessity is required for collection and any processing of any consumer health data, and a regulated entity must obtain separate consent or meet the same necessity standard to share the data."[31] The types of data covered by the act include "'consumer health data,' which has a similarly broad definition, "personal information that is linked or reasonably linkable to a consumer and that identifies the consumer's past, present or future physical or mental health status."[32] The law includes several exceptions, including de-identified data and publicly available information. In addition, the definition of a consumer subject does not include an individual acting in an employment context, and the definition of consumer health data does not include personal information "used to engage in public or peer-reviewed scientific, historical, or statistical research."[33] Finally, there are exemptions for data covered by existing federal statutes such as HIPAA, the Gramm-Leach-Bliley Act, the Social Security Act, the Fair Credit Reporting Act and the Family Educational Rights and Privacy Act.[34] The Washington Act

[28] *See, Protecting Washingtonians' Personal Health Data and Privacy,* Washington State Office of the Attorney General, (2023), *available at*: https://www.atg.wa.gov/protecting-washingtonians-personal-health-data-and-privacy#:~:text=The%20Act%20was%20developed%20to,My%20Health%20My%20Data%20Act.
[29] *Id*.
[30] *Id*.
[31] Amy Olivero and Anokhy Desai, International Association of Privacy Professionals, *Washington's My Health, My Data Act* (April 2023), *available at*: https://iapp.org/resources/article/washington-my-health-my-data-act-overview/.
[32] *Id.*
[33] *Id.*
[34] *Id.*

also requires regulated entities to (i) "maintain a consumer health data privacy policy that clearly and conspicuously discloses how they use the consumer health data, (ii) prohibit the Entities from collecting and sharing consumer health data without the consumers' consent, (iii) empower consumers with the right to confirm and access their own consumer health data, withdraw consent, and have their data deleted, (iv) prohibit the consumer health data from being sold without valid authorization signed by the consumer, and (v) restrict geofencing around in-person health care facilities to identify, track, or send messages to a consumer."[35]

Finally, the Washington statute provides for, in addition to an action bought by the States Attorney General, a *private right of action*, for claimants who are "able to prove the five elements of a WCPA claim, which are (i) an unfair or deceptive act or practice, (ii) occurring in trade or commerce, (iii) public interest impact, (iv) injury to plaintiff in his/her business or property, and (v) causation."[36] A violation of the Washington Act carries a maximum $7,500 civil penalty but the courts also have discretion to increase damage awards up to three times the actual damages sustained or $25,000, whichever is less."[37]

Following the *Washington My Health, My Data Act*, similar statutes were enacted in Nevada and Connecticut.

The *Nevada Health Data Privacy Act* and the *Connecticut Health Data and Child Online Safety Act* also became law in 2023. It has been noted that "[t]hese state laws share a number of similarities, including prohibitions on the collection and sharing of consumer health data without notice and consumer consent, as well as prohibitions on the sale of consumer health data absent written authorization from consumers."[38]

---

[35] John Pavolotsky and Genta Iwasaki, Stoel Rives, LLP, *FAQ: Washington State's, 'My Health Data Act' LEGAL ALERT* (June 9, 2023), *available at*: https://www.stoel.com/legal-insights/legal-updates/faq-washington-state%E2%80%99s-%E2%80%98my-health-my-data-act%E2%80%99.

[36] *Id.*

[37] *Id.*

[38] Amy Cooperstein, Audrey Davis, Alaap B. Shah, Christopher D. Taylor, *Nevada Joins Washington, and Connecticut to Protect Consumer Health Data Privacy,* Epstein Becker Green (July 11, 2023), *available at*: https://www.healthlawadvisor.com/nevada-joins-washington-and-connecticut-to-protect-consumer-health-data-privacy#:~:text=On%20June%2016%2C%202023%2C%20Nevada,effect%20on%20March%2031%2C%202024.

Suggestions for Managing Data Privacy Considering the new Consumer Privacy Laws

Considering the changing consumer data privacy legal environment, new challenges have arisen for entities that are especially acute for entities operating in multiple jurisdictions. As a preliminary matter, entities should understand the jurisdictional laws applicable to the entity and the applicable revenue thresholds to determine the state laws to which the entity may be subject as well as the sufficiency of the entities privacy policies to address the same. An entity should also seek to understand their role regarding personal data as defined by the law (e.g., processor or controller) and special attention should be paid to an entity's data collection activity, consumer consent, retention and destruction policies as well as any arrangement whereby data is sold or provided to third party data processors or other business partners.

It is also advisable that an entity evaluate its privacy program annually; a questionnaire or checklist can help analyze the data within an organization and also help document the flow of data both within and outside the organization.

The Society for Human Resource Management ("SHRM") has recommended several steps for compliance with the CCPA as amended, in the context of human resources information, which may be instructive for compliance with consumer data privacy laws in general. The SHRM recommendations include, (i) inventory and map of all consumer data, including employee and job applicant data; (ii) take appropriate steps to secure all consumer and employment-related data; (iii) prepare and provide a 'notice at collection' to all consumers, including employees and job applicants, at or before collecting any consumer data; (iv) prepare and post a comprehensive privacy policy on your website; (v) deploy a process to receive and respond to consumer requests from all consumers, a process referred to by many privacy practitioners as a DSR or data subject request; (vi) implement data minimization rules; and (vii) train all managers and employees on all [the Acts] requirements in which they play any role.[39]

[39] *See*, Usama Kahf, Darcey M. Groden, Anne Yarovoy Khan, Jenna Rogenski, Christoper M, Champine, Anthony Isola and Benjamine M. Ebbink, *Seven Steps to Comply with the CCPA,* Society for Humay Resource Management (May 31, 2023), *available at*: https://www.shrm.org/resourcesandtools/legal-and-compliance/state-and-local-updates/pages/california-ccpa-data-privacy.aspx.

The consumer data privacy legislation trend represents a new and growing dynamic for entities that collect, process, or store consumer data. Considering the emerging consumer data privacy environment, it is more important than ever that entities employ sound data management practices and continually monitor their legal environment to ensure compliance with the new laws. It is equally important that entities ensure that measures are in place to address financial risks posed by these laws including cyber insurance and other risk transfer mechanisms.