HINSHAW

Alerts

Q&A: Four State Data Privacy Compliance Insights for 2024

February 9, 2024
Privacy, Cyber & AI Decoded

With the first month of 2024 now behind us, it is time for organizations to start seriously considering key comprehensive state data privacy compliance obligations for 2024.

In total, seven states passed data privacy laws in 2023, which will require some degree of compliance on the part of covered businesses this year:

- Montana Consumer Data Privacy Act (*eff*. Oct. 1, 2024)
- Florida Digital Bill of Rights (*eff*. July 1, 2024)
- Texas Data Privacy and Security Act (*eff*. July 1, 2024)
- Oregon Consumer Privacy Act (*eff*. July 1, 2024)
- Delaware Personal Data Privacy Act (*eff*. Jan. 1, 2025)
- Iowa Act Relating to Consumer Data Protection (*eff*. Jan 1, 2025)
- New Jersey Data Privacy Act (*eff*. Jan. 15, 2025)

Q: What Should Privacy Teams Consider First?

A: Does the law apply to your organization, and if so, how? The threshold requirements of these state laws are not mirror images. Organizations should first determine if they fall within the umbrella of these new laws or an exemption.

- For example, the Texas Data Privacy and Security Act (TDPSA) applies to organizations that conduct business in the state or produce products or services that are consumed by Texas residents, process or engage in the sale of personal data, and do not identify as a "small business," as that term is defined by the United State Small Business Administration (SBA).

While seemingly simple, small businesses may find making this threshold determination challenging because there is no one definition of a small business under the SBA regulations. Instead, the definition varies by industry.

- Oregon's Consumer Privacy Act has a limited data-related exemption for financial companies falling under GLBA requirements, although there is an exemption for a bank holding company. Businesses should consider what this means for their non-GLBA data businesses.

Attorneys

Cathy Mulrow-Peattie

Jason J. Oliveri

Service Areas

Privacy, Security & Artificial Intelligence

Q: Do I Need to Adjust my Data Privacy Notices and Data Subject Access Rights Request Form?

A: Many organizations have in place a privacy notice compliant with existing federal and state laws about the categories of personal information being processed, the purposes of processing, and the means by which data subjects can submit requests to exercise their data subject rights.

- In addition to these now standard disclosures, covered businesses who also engage in targeted advertising must clearly and conspicuously disclose such processing to consumers and what entities they share targeted advertising personal data with.
- The TDPSA has specific disclosure requirements for the sale of sensitive and biometric information.
- Notably, Montana, Texas, Delaware, Oregon, and New Jersey have joined Colorado, Connecticut, and California in requiring that covered businesses provide consumers with a universal opt-out or global privacy control for the sales of personal data or the use of personal data in targeted advertising. In other words, the goal is to provide a method for consumers to control their privacy preferences across various websites instead of opting out on a controller-by-controller basis. Montana and Texas require compliance with this requirement to be operational by January 1, 2025; New Jersey by July 15, 2025; and Delaware and Oregon by January 1, 2026. Connecticut and Colorado's universal opt out requirements must be complied with this calendar year. Covered businesses should consider a multi-state implementation process despite the statutory differences.

Connecticut and California Attorney General's offices have issued notices of violations and brought enforcement actions against a wide variety of industries over the lack, inadequate, and confusing privacy disclosures and data subject rights mechanisms.

California's Attorney General in the Sephora case also enforced on the failure to implement a global privacy control. Please note that we expect the growth of privacy enforcement actions on notice and opt-out requirements in 2024 in these states with comprehensive privacy laws.

Q: Have the Requirements for Sensitive Data Use Expanded?

A: Each new privacy law referenced above also requires that covered businesses must obtain consumer consent before processing sensitive information. Again, what is defined as sensitive data varies across states.

The Oregon Consumer Privacy Act covers, for example, the status as "transgender or nonbinary" and "as a victim of crime."

The New Jersey Data Privacy Act has an expansive definition of sensitive personal data, which includes financial information and precise geolocation data.

Across the numerous states with precise geolocation data defined as sensitive data, e-commerce businesses or businesses with store or office locators should confirm if their websites or applications are collecting this information.

Colorado's Attorney General has already sent letters to organizations emphasizing compliance obligations relating to the collection and use of sensitive data. California's Attorney General and the Federal Trade Commission have already brought enforcement actions on sensitive data and location data consent requirements. We expect this to be another key enforcement area going forward.

Q: What is New for Vendor or Processor Contracts?

A: With more comprehensive state privacy laws on the books, businesses that work with third-party service providers will need to ensure that the relationship is governed by an enforceable contract that complies with these new state laws.

Some additional requirements under these state privacy laws include the following:

- Each person processing personal information is subject to a duty of confidentiality and the processing purposes should be limited;
- The vendor deletes or returns all personal information to the business, as requested at the conclusion of the contract, unless the vendors' retention of the information is required by law;
- The vendor includes an audit requirement that makes available to the business all information in the vendor's possession necessary to demonstrate the vendor's compliance with the law; and
- The vendor engages any subcontractor pursuant to a written contract that requires the subcontractor to meet the obligations of the vendor with respect to the personal information.

Under certain state and federal cybersecurity laws, businesses should conduct due diligence before engaging a potential vendor in order to understand their security practices as to personal data.

Also, do not forget to loop in your artificial intelligence compliance team when retaining an AI vendor. Retaining the wrong vendor could result in consumer lawsuits, regulatory investigations or security breaches and may ultimately cause reputational and commercial harm to the business.

Given the need to prioritize privacy compliance, service provider contracts often fall to the bottom of the compliance list, but we recommend that organizations put data processing agreements in place to reduce this gap. Unfortunately, the California Attorney General has already enforced this gap.

What's Next?

Complying with one state privacy law does not necessarily mean compliance with all. They all have their nuances. Businesses already familiar with and compliant with the data privacy laws in California, Colorado, Connecticut, and Virginia will likely need to make adjustments to their existing compliance programs.

For those drafting new policies with a look to the future, we recommend that you consider that the number of comprehensive state privacy laws will continue to grow, with New Hampshire's to be signed shortly by Governor Sununu. For more insights into Hinshaw's predictions for 2024, see Marking Data Privacy Week With Four 2024 Predictions.