Comprehensive Consumer Privacy Laws: A Growing Challenge for PEOs

Insights
12.17.24

Comprehensive consumer privacy laws are rapidly expanding across the United States, significantly impacting PEOs. Currently, 19 states have enacted privacy laws, with eight already in effect and 11 set to take effect between January 2025 and January 2026. Here, we breakdown what PEOs need to know about thresholds for applicability and practical steps for compliance.

Key Privacy Principles for PEOs to Keep in Mind

These consumer privacy laws share several core principles:

1. Transparency: Companies must be transparent about how they collect, use, and share consumer data.

2. Control: Consumers should have control over their personal data, including the ability to access, correct, and delete it.

3. Proportionality and Data Minimization: Companies should only collect and retain the minimum amount of data necessary to fulfill specific purposes.

How PEOs Determine Applicability

To determine whether a PEO is subject to a specific state's privacy law, several factors are considered:

- **Doing Business**: A PEO may be doing business in a state if it has a physical presence, worksite employees, or actively targets customers in the state.
- **Consumer Data Thresholds**: Most states have thresholds for the law to apply based on the number of consumers whose data is processed. These thresholds vary but can be easily exceeded, even with relatively low website traffic. California has a unique revenue-based threshold, meaning if your company made over $25 million in gross revenue from anywhere in the world in the last calendar year, your PEO meets the threshold.

Understanding Exemptions and the "Consumer" Definition

Certain types of data and entities may be exempt from privacy law requirements. These exemptions typically relate to data regulated by specific federal laws, such as the Gramm-Leach-Bliley Act (GLBA), HIPAA, or FCRA.

The definition of "consumer" varies by state, but generally includes residents of the state acting in an individual or household capacity. Notably, California's definition extends to employees of PEO customers and their dependents.

Prioritizing Compliance

To effectively manage privacy compliance, PEOs should prioritize the following areas:

- **Transparency**: Develop clear privacy policies and communicate them to consumers and worksite employees.
- **Control**: Implement robust data subject rights processes, including the ability to access, correct, and delete data.
- **Proportionality and Data Minimization**: Conduct regular data audits to identify and eliminate unnecessary data collection and retention practices.

As the privacy landscape continues to evolve, PEOs must stay informed and adapt their practices to ensure compliance with these increasingly stringent regulations.

Understanding State-Specific Requirements

While many consumer privacy laws share common requirements, several states have unique provisions. For instance, California's law extends to worksite employees, employees, job applicants, independent contractors, and business-to-business contacts. Additionally, regulations set to take effect in Colorado will soon impose restrictions on the collection of biometric information from employees.

Beyond comprehensive consumer privacy laws, other laws pose significant risks. In California, over 1,100 lawsuits have been filed since June 2022, alleging violations of the California Invasion of Privacy Act (CIPA) due to the sharing of user data with third parties through cookies and tracking technologies. Similarly, the federal Video Privacy Protection Act (VPPA) protects video viewing history, potentially impacting the use of embedded video platforms like YouTube and Vimeo. Illinois' Biometric Information Privacy Act (BIPA) has also been a source of significant litigation over the years.

Practical Steps for Compliance

The adage "you can't protect what you don't know you have" is particularly relevant to data privacy. Creating comprehensive data asset inventory can provide valuable insights into your organization's

data collection and usage practices.

A well-crafted privacy policy is essential for both legal compliance and customer trust. It should clearly communicate your data practices, going beyond the bare minimum requirements of consumer privacy laws.

A data retention policy is crucial for complying with data minimization principles and managing consumer expectations. It should outline clear guidelines for data retention and deletion. Implementing a robust process for handling consumer rights requests is essential. This process should be accessible to all consumers, including those who may not have regular computer access.

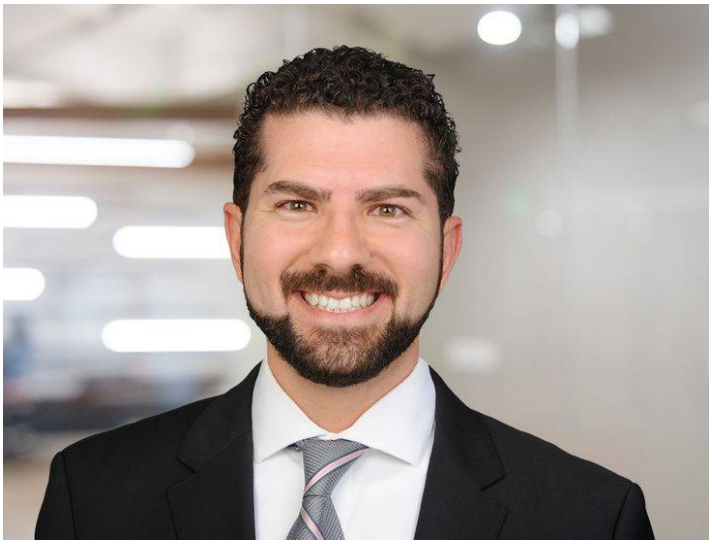
Conclusion: Proactive Action is Key

If you're uncertain about the applicability of consumer privacy laws to your PEO and your customers, take the initiative to assess your exposure. By understanding your obligations and taking proactive steps to comply, you can mitigate risks and protect your business.

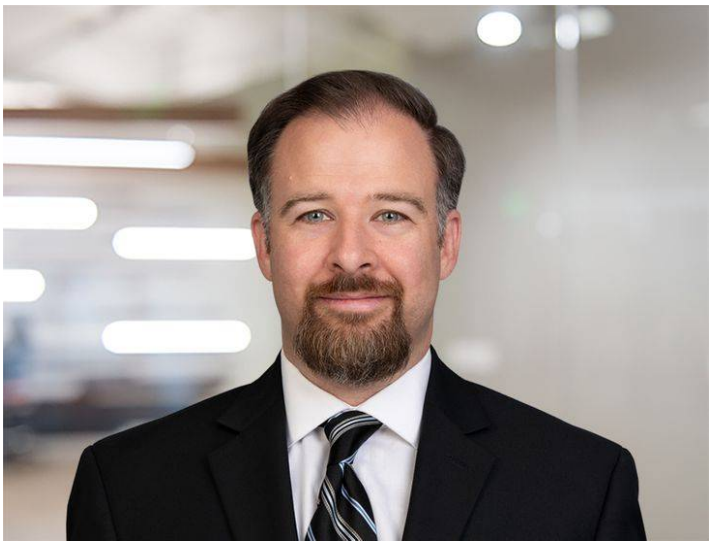
Make sure you are subscribed to Fisher Phillips' Insight system to get the most up-to-date information. We will continue to monitor the situation and provide updates as more information becomes available. Any questions may be directed to your Fisher Phillips attorney, the authors of this Insight, or any attorney in our PEO Advocacy and Protection Team.

This article is reprinted with permission from PEO Insider where it appeared in the December 2024 edition, available here.

Related People



Usama Kahf, CIPP/US
Partner
949.798.2118
Email



Kile E. Marks, FIP, CIPP/US, CIPM, CIPT
Associate
858.964.1582
Email

Service Focus

Privacy and Cyber

Industry Focus

PEO Advocacy and Protection