DAVIS GILBERT

Privacy + Data Security

2024 Privacy Issues: New Laws & Requirements Reshape Compliance

The Bottom Line

- Businesses must navigate an increasingly complex and varied privacy regulatory environment, with differing laws across multiple regions creating compliance challenges.
- New regulations at both the local and global levels necessitate continual adaptation and updating of privacy practices and policies.
- As more consumer privacy and data laws take effect, businesses should work closely with trusted privacy law attorneys to ensure compliance.

As we step into 2024, the privacy regulation landscape continues to evolve rapidly, presenting significant challenges for businesses. We're seeing more privacy laws from individual states, which creates a complex web of compliance requirements across different regions. Additionally, new data broker registration laws, notably the California Delete Act, and the EU-U.S. Data Privacy Framework, are reshaping how data is handled. These developments underscore the importance for businesses to stay informed and agile in their privacy strategies.

1. Continued Proliferation of State Privacy Laws

State comprehensive consumer privacy laws have moved beyond California, as Virginia, Colorado, Connecticut and Utah all joined the fray last year. In 2024, we will see recently enacted laws take effect in three more states – Montana, Oregon and Texas, along with more states following in 2025 and 2026. With each new state law, the disconnects between them continue to grow. For example, not all the states' privacy laws require the same disclosures and they even define key terms differently, such as what "sensitive personal information" means. Further, there is no one "strictest standard" to aim for, so compliance is becoming more challenging. No business can rest on its laurels when it comes to privacy programs.

2. New Data Broker Registration Laws and the California Delete Act

There are now four states with data broker registration laws in effect: California, Vermont, Oregon and Texas. While the California and Vermont registries have been in effect for some time, the Oregon and Texas registries are expected to be launched in early 2024. Most of the data broker registration laws merely require providing certain information, such as a company's contact information and a link to its privacy policy, as well as a fee to appear on a publicly accessible registry. However, California took this to a whole new level by enacting the California "Delete Act."

The Delete Act will require integration between the state registry and the data broker's systems so that California consumers can opt-out of all registered data brokers with one simple click. Thereafter, data brokers will be required to refresh those deletion requests every 45 days – essentially making deletion permanent. The state has two years to create this mechanism, which would take effect in mid-2026. And starting in 2028, data brokers will be required to undergo an audit by an independent third party to verify compliance.

3. EU-U.S. Data Privacy Framework for Cross Border Data Transfers

The European Commission adopted an adequacy decision on the EU-U.S. Data Privacy Framework (DPF), which will provide an additional mechanism to ensure the lawful transfer of data across the Atlantic. The long-awaited announcement, culminating after a series of negotiations between the EU and the U.S., followed the EU high court's 2020 decision overturning the DPF's predecessor, the EU-U.S. Privacy Shield Framework. U.S. companies that are certified under the DPF will no longer need to implement Standard Contractual Clauses or Binding Corporate Rules for data transfers or conduct a Transfer Impact Assessment. To join the DPF, companies must complete a self-certification process through the U.S. Department of Commerce and meet other criteria, such as updating their privacy policies and providing independent recourse mechanisms for EU data subjects to submit complaints for investigation.

4. Issue-Specific Laws, Such as Washington's My Health My Data Act

Washington's My Health My Data Act (MHMD Act), the first consumer privacy law focused on health data, takes effect on March 31, 2024. The MHMD Act regulates "consumer health data," which is 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 (including specific categories that fall under this designation). Unlike existing consumer data privacy laws, the MHMD Act does not contain a revenue or records threshold. It broadly applies to any entity that conducts business in Washington or provides products and services to consumers in Washington or to non-Washington residents who interact with regulated entities in the state. The MHMD Act provides exemptions for HIPAA-covered entities and other types of regulated data.

Regulated entities will need to ensure their privacy policies include the required disclosures and review consent practices based on their data processing and/or sharing activities. Any regulated entity that sells consumer health data must obtain the consumer's valid authorization to do so and retain a copy of the authorization for six years. Like existing data privacy laws, regulated entities must implement reasonable and appropriate security controls for consumer health data and execute DPAs with data processors. The MHMD Act carries statutory damages and includes a private action, giving it some of the stiffest penalties among any existing consumer data privacy law.

5. Industry Initiatives to Comply with New Privacy Laws

For over a year, industry initiatives — many led by the Interactive Advertising Bureau (IAB) — have been attempting to address compliance issues that arose with the advent of more and more privacy laws. At the forefront of this effort is the IAB Multi-State Privacy Agreement (MSPA), an industry contractual framework originally intended to aid advertisers, publishers, agencies and ad tech intermediaries in complying with the initial five state privacy laws. It became effective in 2023, replacing a predecessor initiative focused only on California.

The IAB is now updating the MSPA to include eight new states that have recently enacted consumer privacy laws. The MSPA is not a "model contract" or a template agreement; instead, it is a set of privacy-protective terms that spring into place among a network of signatories and that follow the data as it flows through the digital ad supply chain. In addition, the IAB recently established a voluntary Accountability Program as part of its MSPA compliance framework. Through the Accountability Program, MSPA Signatories have an opportunity to earn an 'MSPA Certified' seal after demonstrating how they comply with the MSPA's requirements. The IAB is also leading the charge to develop several technical standards to aid in compliance, including the Global Privacy Platform (GPP).

Privacy + Data Security

For More Information

Please contact the attorneys listed below or the Davis+Gilbert attorney with whom you have regular contact.

Richard Eisert

Partner
212 468 4863
reisert@dglaw.com

Gary Kibel

Partner
212 468 4918
gkibel@dglaw.com

Zachary Klein

Associate
212 237 1495
zklein@dglaw.com

Jeremy Merkel

Associate
212 468 4976
jmerkel@dglaw.com