

# New Year, New Privacy Laws!

2025 ushers in a new administration in addition to several new or revised state consumer privacy laws. Below, we have outlined these developments.

## Comprehensive Consumer Privacy Laws

States continued to pass comprehensive consumer privacy laws throughout 2024. 2025 brings eight new state-level comprehensive consumer privacy laws into effect. As with the five state privacy laws that [went into effect in 2024](#), states continue to introduce nuances as to applicability thresholds, entity and data level exemptions, and other compliance requirements for subject companies.

Companies should evaluate current compliance programs and whether they are staying current with new use cases involving personal information.

Organizational privacy compliance priorities may include:

- Analyzing state law thresholds for applicability.
- Revising privacy notices to account for new notice requirements or consumer privacy rights.
- Implementation of consumer preference centers and recognition of universal browser mechanisms such as Do Not Track and Global Privacy Control browser signals.
- Evaluation (or implementation) of data processing agreements for inclusion of statutorily required elements.
- Vigilance in data mapping/asset inventory maintenance for capturing all personal information processing activities and expanded data types that may qualify as personal information.

The eight states with 2025 effective dates are provided below along with links to more information.

- [Delaware](#) (January 1, 2025)
- [Iowa](#) (January 1, 2025)
- [Nebraska](#) (January 1, 2025)
- [New Hampshire](#) (January 1, 2025)
- [New Jersey](#) (January 15, 2025)
- [Tennessee](#) (July 1, 2025)
- [Minnesota](#) (July 31, 2025)
- [Maryland](#) (October 1, 2025) (certain provisions only apply to data processing activities after April 1, 2026)
  - The Maryland Online Data Privacy Act ([MODPA](#)) includes novel provisions not found in other state consumer privacy laws. Entities subject to MODPA may need to modify their compliance programs accordingly. Most significantly, MODPA has strict requirements related to sensitive data. MODPA prohibits the collection or processing of sensitive data unless *strictly necessary* to provide or maintain a specific product or service requested by the consumer (even if consent is granted). MODPA also includes an outright ban on the sale of sensitive data.

Although Oregon's consumer privacy law went into effect as of July 1, 2024, **as of July 1, 2025**, the [Oregon Consumer Privacy Act](#) **applies to most nonprofits**. Oregon, Colorado, and Delaware are unique in their application to nonprofits whereas remaining states with comprehensive

consumer privacy laws currently in effect largely exempt nonprofits from their orbit for most personal information processing activities.

## Global Privacy Control Recognition

Universal opt-out mechanisms (UOOMs), including global privacy controls (GPCs), indicate a consumer's choice to opt out of certain tracking technologies that an entity might use for purposes of targeted advertising or profiling. **January 1, 2025**, marks the date upon which entities subject to the consumer privacy laws enacted in [Connecticut](#), [Montana](#), and [Texas](#) must recognize such browser signals.

## Neural and Biometric Data

Certain types of data continue to gain attention, including “neural” data as a form of sensitive personal information that may require affirmative opt-in consent prior to processing activities.

### California

- **Effective as of January 1, 2025**, California's [A.B. 1008](#) and [S.B. 1223](#) amend the California Consumer Privacy Act of 2018 to include “neural” data. California defines neural data to include “information that is generated by measuring the activity of a consumer's central or peripheral nervous system, and that is not inferred from nonneural information.”

### Colorado

- **Effective as of August 6, 2024**, Colorado's [House Bill 24-1058](#) amends the Colorado Privacy Act to include neural data as a form of sensitive personal information subject to regulation and enforcement under the Colorado Privacy Act. House Bill 24-1058 defines neural data as “information that is generated by the measurement of the activity of an individual's central or peripheral nervous systems and that can be processed by or with the assistance of a device.”
- **Effective July 1, 2025**, Colorado's [HB24-1130](#) amends the Colorado Privacy Act to add definitions for “biometric data” and “biometric identifiers.” HB24-1130 establishes new requirements for subject entities, including requiring prior consent from a consumer *before* collecting biometric data. Additionally, HB24-1130 creates specific regulations applicable to the processing of an *employee's* biometric data.

## Looking Forward

In addition to comprehensive consumer privacy laws coming into effect this year, Indiana, Kentucky, and Rhode Island all have similar laws on the books that come into effect beyond 2025. Creating an effective compliance program for consumer data privacy laws is likely to become even more important as the number of regulatory agencies and regulatory obligations increase.

Our team will continue to monitor data privacy developments through the upcoming year under the incoming administration. If you have any questions about the dynamic consumer data privacy space and how upcoming requirements could affect your business, please contact the authors.