

State Privacy Bingo

By Matthew H. Meade and Elizabeth Wilson

STATE PRIVACY LEGISLATIVE UPDATE AS OF AUGUST 2023

The first half of 2023 has been busy for state privacy legislation. As of August 9, 2023, eleven states¹ have passed consumer privacy laws. Delaware may soon become the 12th state if Governor Carney signs the recently passed Delaware Personal Data Privacy Act. Four states still have pending privacy bills in the running for this year. Please see below for a snapshot of the state privacy law landscape for August and practical tips you can employ to comply with these new laws.

STATES WITH PASSED COMPREHENSIVE PRIVACY LAWS

(As of August 9, 2023) - States in red are currently in effect.

- **California** - [California Privacy Rights Act](#)
- **Colorado** - [Colorado Privacy Act](#)
- **Connecticut** - [Connecticut Data Privacy Act](#)
- **Delaware** - [Delaware Personal Data Privacy Act](#) – if signed into law, will take effect on Jan. 1, 2025²
- **Indiana** - [Indiana Consumer Data Protection Act](#) – in effect as of Jan. 1, 2026³
- **Iowa** - [Iowa Consumer Data Protection Act](#) – in effect as of Jan. 1, 2025
- **Montana** - [Montana Consumer Data Privacy Act](#) – in effect as of Oct. 1, 2024
- **Oregon** - [An Act Relating to Protections for the Personal Data of Consumers](#) – in effect July 1, 2024 (for for-profits)⁴
- **Tennessee** - [Tennessee Information Protection Act](#) – in effect as of July 1, 2025
- **Texas** - [Texas Data Privacy and Security Act](#) – in effect as of July 1, 2024⁵
- **Utah** - [Utah Consumer Privacy Act](#) in effect as of December 31, 2023
- **Virginia** - [Virginia Consumer Data Protection Act](#)

¹ Florida has also adopted the [Florida Digital Bill of Rights](#) that will be in effect as of July 1, 2024, however the law is narrowly tailored so that it applies to only a handful of companies who (i) have an annual revenue of over \$1 billion dollars and (ii) satisfies one of the following: (a) derives 50% or more of its revenue from the sale of advertisements; (b) operates a consumer smart speaker and voice command component service with an integrated virtual assistant connected; or (c) operates an app store or a digital distribution platform that offers at least 250,000 different software applications for consumers to download and install.

² If this Act is enacted before or on January 1, 2024, this Act takes effect on January 1, 2025. If this Act is enacted after January 1, 2024, this Act takes effect on January 1, 2026.

³ Chapter 11 Section 2, pertaining to the responsibilities of the Attorney General's office, is already in effect.

⁴ Most provisions become operative on July 1, 2024, but the privacy opt out signal requirements are delayed until January 1, 2026. Sections 1 to 9 of the law are not operative for non-profit organizations until July 1, 2025.

⁵ Requirements to recognize universal opt outs will be in effect on January 1, 2025.

STATES WITH PENDING PRIVACY BILLS

(As of August 9, 2023)

- **Massachusetts**
 - [Massachusetts Data Privacy Protection Act \(H.83 / S.25⁶\)](#)
 - *Current Status:* Referred to Committee on Feb. 16, 2023.
 - [Massachusetts Information Privacy and Security Act \(H.60 / S.227⁷\)](#)
 - *Current Status:* Referred to Committee on Feb. 16, 2023.
 - [Internet Bill of Rights \(H.1555\)](#)
 - *Current Status:* Referred to Committee on Feb. 16, 2023.
- **New Jersey**
 - [New Jersey Disclosure and Accountability Transparency Act \(S.3714 / A.505\)⁸](#)
 - *Current Status:* Referred to Committee on March 13, 2023.
- **North Carolina**
 - [North Carolina Consumer Privacy Act \(SB 525\)](#)
 - *Current Status:* Referred to the Committee on April 4, 2023.
- **Pennsylvania**
 - [Consumer Data Privacy Act \(HB 1201\)](#)
 - *Current Status:* Referred to the Committee on May 19, 2023.
 - [Consumer Data Protection Act \(HB 708\)](#)
 - *Current Status:* Referred to the Committee on March 27, 2023.

WHAT YOU CAN DO TO PREPARE

There are several steps companies can take to ensure compliance with these new and upcoming state laws. Such steps may include the following:

- Complete a scoping analysis to see which state laws are triggered by your company's data processing⁹ activities. Most states have scoping triggers based on doing business in the respective state and meeting certain revenue and/or processing volume thresholds, but there are exceptions to this general rule (e.g., Texas).
- Complete a data map describing your data processing activities. The data map may include, for example: (a) the types of individuals and data attributes connected to the personal data your company processes; (b) the purposes for processing the personal data; (c) who is the personal data being shared with and for what purpose; and (d) where and how long is personal data being retained.
- Review and/or revise your organization's vendor contract templates to include required contractual terms under new state privacy laws. To the extent required, complete contract remediation exercises to update privacy terms in existing vendor agreements.
- Review and/or revise your external facing privacy documents including any consents, privacy policies, notices and/or terms of use to include new state privacy law requirements.
- Review and/or revise your organization's internal privacy policies and procedures, including, for example, your data subject request, cybersecurity, data retention and data handling policies.



This Cybersecurity, Data Protection & Privacy Alert is intended to keep readers current on developments in the law and is not intended to be legal advice. If you have any questions, please contact Matthew H. Meade at 412.566.6983 or mmeade@eckertseamans.com, Elizabeth Wilson at 215.851.8497 or ewilson@eckertseamans.com, any attorney in our Cybersecurity, Data Protection & Privacy Practice Group, or any other attorney at Eckert Seamans with whom you have been working for further information and assistance.

⁶ Bills H.83 and S.25 are substantively the same.

⁷ Bills H.60 and S.227 are substantively the same.

⁸ Bill S3714 and A505 are identical.

⁹ Processing activities may include the collection, use, access, disclosure, and/or retention of personal data.