

New US State Privacy Laws Taking Effect in 2025

Publications

January 2025

By: Madeleine Findley, Xinyue Lu

As we enter a new year, the patchwork of US privacy laws continues to expand and become more complex. With the change in control of the White House and Congress, the prospects for a federal privacy law have grown even less likely. State legislatures have been actively considering and adopting privacy laws, and we expect that activity will increase. Over the course of 2025, eight new state consumer privacy laws will take effect. Laws in four states—Delaware, Iowa, Nebraska, and New Hampshire—will take effect on January 1, and a law in New Jersey will take effect on January 15. Laws in Tennessee and Minnesota will take effect in July, and a law in Maryland will take effect in October. We offer an overview of some key similarities and differences between these laws and what they mean for privacy compliance in the United States.

The 2025 laws largely align with existing privacy frameworks and will look familiar to businesses that already comply with the consumer privacy laws in states such as California, Connecticut, Colorado, Texas, or Virginia. The new laws require businesses to maintain privacy notices, have written contracts with third-party processors, observe data minimization principles, and implement security measures to safeguard personal data. Consumers in these states will also have the right to access, obtain copies of, and delete their personal data, as well as to opt out of targeted advertising and the sale of their personal data. These new laws, except for Iowa's, also allow consumers to request corrections of their personal data and opt out of certain profiling in furtherance of automated decisions. Processing sensitive personal data will require prior opt-in consent, except in Iowa, where the law requires notice and an opportunity to opt out.

Several novel aspects appear in the 2025 privacy laws that will require additional compliance planning and may impose additional, sometimes differing requirements. These reflect a growing trend at the state level: adopting additional privacy protections or modifying certain definitions to further limit data collection and use. Businesses should monitor these trends, which we anticipate will continue and become ever more challenging to manage.

- Businesses will have to honor consumer opt-out preference signals or universal opt-out mechanisms under six of the 2025 laws (in Nebraska, Delaware, New Hampshire, New Jersey, Minnesota, and Maryland).

- States are adding new provisions to their definitions of “sensitive personal data,” such as neural data, biological data, transgender or nonbinary status, financial information, pregnancy, and national origin.
- Requirements for data minimization are becoming more prescriptive and limiting. For example, the Maryland Online Data Privacy Act imposes a novel “strictly necessary” data minimization requirement that significantly limits businesses’ ability to use sensitive data for purposes other than providing a specific product or service requested by the consumer, and it prohibits all sale of sensitive data and the data of children under the age of 18 (regardless of consent).
- Activities that profile consumers will receive closer regulatory attention. The Minnesota law expands consumers’ rights to know about profiling. It allows consumers to question the results of such profiling, understand the reasons for decisions made based on profiling, and learn what actions they could have taken to alter those decisions.

Regulatory enforcement activity is likewise expected to increase in 2025—even in states without comprehensive consumer privacy laws—as state attorneys general open inquiries under these and state consumer protection laws. The new year is sure to bring other developments in privacy law; including an increased focus on automated decision-making and artificial intelligence, data brokers, and targeted advertising.

This article is available in the Jenner & Block Japan Newsletter. / この記事はJenner & Blockニュースレターに掲載されています。

Related Attorneys



Madeleine Findley

Partner

mfindley@jenner.com

+1 202 639 6095



Xinyue Lu

Associate

xlu@jenner.com

+1 202 637 6376

Related Articles

Jenner & Block Japan Newsletter | January 2025

Related Capabilities

Data Privacy and Cybersecurity

Japan Practice

© 2026 Jenner & Block LLP. Attorney Advertising. Jenner & Block LLP is an Illinois Limited Liability Partnership including professional corporations. This publication, presentation, or event is not intended to provide legal advice but to provide information on legal matters and/or firm news of interest to our clients and colleagues. Readers or attendees should seek specific legal advice before taking any action with respect to matters mentioned in this publication or at this event. The attorney responsible for this communication is Brent E. Kidwell, Jenner & Block LLP, 353 N. Clark Street, Chicago, IL 60654-3456. Prior results do not guarantee a similar outcome. Jenner & Block London LLP, an affiliate of Jenner & Block LLP, is a limited liability partnership established under the laws of the State of Delaware, USA and is authorised and regulated by the Solicitors Regulation Authority with SRA number 615729. Information regarding the data we collect and the rights you have over your data can be found in our Privacy Notice. For further inquiries, please contact dataprotection@jenner.com.

Stay Informed

