Now & Next
Privacy and Technology Alert

February 23, 2026

US state privacy laws require privacy assessments

By Jacqueline Cooney, Jenny Holmes, and Hannah Edmonds

As state privacy rules multiply, knowing your data and its risks has never been more important.

What's the impact?

- As US state privacy laws continue to expand, companies must increasingly navigate mandatory privacy assessments tied to specific data-processing activities.
- Regulators can request these assessments at any time, organizations need accurate, regularly updated documentation of how personal data is collected, used, shared, and risk-managed.
- With eighteen state privacy laws now imposing assessment requirements, building a scalable, internal privacy assessment function has become essential for operational compliance.

For companies grappling with the ever-evolving patchwork of US state privacy laws, an important consideration is that many of those laws require undertaking privacy assessments under certain circumstances. Those assessments have varied names, including "data protection assessments," "data protection impact assessments," "risk assessments," or "data privacy and protection

assessments"—but they all mean one thing: knowing what data is collected, used, and shared, as well as the risks associated with those activities is becoming increasingly important in the US.

Whether a company must conduct a privacy assessment is based not just on whether any state privacy laws are applicable to it, but also on the types of personal data processing activities that the organization engages in. When an organization is required to complete privacy assessments, those assessments must be available for review by regulatory authorities upon request and should therefore be accurate and updated regularly.

Out of the nineteen (19) states with effective comprehensive privacy laws, seventeen (17)[1] impose some kind of privacy assessment. Additionally, though we tend to not consider the Florida Digital Bill of Rights (FDBR) a comprehensive privacy law due to its narrower scope, it also imposes a privacy assessment requirement. So, in total, as of the date of publication of this article, eighteen (18) state privacy laws must be considered as companies build their internal privacy assessment functions.

Privacy assessment requirements are triggered by high-risk processing activities

As with all privacy law compliance evaluations, we recommend that companies first determine whether a state privacy law applies to them—thresholds vary across states depending on the number of residents whose data is processed, whether the company is an exempt small business, or, as in the case of California, whether the revenue is above a certain threshold.

If a state privacy law is applicable to a company, then the requirement for that company to complete a privacy assessment is mainly triggered by whether that company conducts high-risk processing activities,[2] which are sometimes referred to as personal data processing activities that pose a "heightened risk of harm" to individuals, such as:

- processing for targeted advertising
- selling personal data
- processing sensitive data
- processing personal data for profiling or with automated decision-making technology (ADMT)

---

[1] States that require organizations to conduct privacy assessments include Virginia, Colorado, Connecticut, Texas, Delaware, Oregon, Indiana, Montana, New Jersey, New Hampshire, Nebraska, Tennessee, Minnesota, Maryland, Kentucky, Rhode Island, California, and Florida.

[2] Additionally, the Delaware Personal Data Privacy Act (DPDPA) only applies its privacy assessment requirement to companies conducting high-risk processing activities of personal data of at least 100,000 Delaware consumers, excluding data controlled solely for completing payment transactions.

- other processing activity that may pose a heightened risk of harm to individuals

Organizations generally must conduct privacy assessments before beginning any high-risk data processing activities. We provide further context and details on each of these processing activities below.

PROCESSING FOR TARGETED ADVERTISING

Processing for targeted advertising happens when a company engages in direct advertising activities, including through the use of tracking technologies. Specifically, this occurs when a company provides specific advertisements to a consumer or a defined audience based on demographics, preferences, interests, characteristics, or other information the company has collected or inferred about those consumers such as through cookies or interactions of the consumers on non-affiliated websites.

SELLING PERSONAL DATA

Selling personal data involves an exchange of personal data for monetary or other valuable consideration. Many states' definition of "sale" or "selling" are typically broad in scope and can often include sharing for advertising and analytics purposes. For example, under the California Consumer Privacy Act (CCPA), the selling of personal information means "selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by a business to a third-party for monetary or other valuable consideration." The Virginia Consumer Data Protection Act (VCDPA) takes a more limited approach, defining the sale of personal data to be the exchange of personal data for monetary consideration by the controller to a third party.

PROCESSING SENSITIVE DATA

Processing sensitive data means processing any data defined as "sensitive" under any of the applicable state privacy laws. Sensitive data can include, but is not limited to, Social Security number, passport number, racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, citizenship, immigration status, genetic or biometric data, children's data, and precise geolocation data. Notably, recent amendments to a few of the state privacy laws, including those of California, Colorado, and Connecticut (effective July 1, 2026), now deem neural data as sensitive data as well.

PROCESSING PERSONAL DATA FOR PROFILING OR WITH ADMT

Processing personal data for profiling generally entails the automated processing of personal data to analyze or predict aspects of a person's life concerning things like health, personal preferences, behavior, etc. Processing personal data with ADMT involves using artificial

intelligence, machine learning, or algorithms to analyze personal data to evaluate, predict, or make significant decisions about a consumer that could have a legal effect on the consumer without, or with limited, human intervention. Examples of decisions that have legal effect include decisions about hiring or lending to a consumer. Processing personal data for profiling or with ADMT is heavily regulated due to the potential for this processing activity to significantly impact consumers' lives regarding employment, housing, or financial services.

What to include in privacy assessments

The state privacy laws generally require organizations to include the following in privacy assessments:

- A description of the processing activity that the privacy assessment is intended to cover
- Explanations regarding how personal data involved in the processing activity is collected, used, stored, shared with/sold to third parties
- A risk analysis that identifies potential risks to consumers related to the processing activity covered, which should include organizational safeguards in place to mitigate those identified risks
- A benefits analysis identifying and explaining direct/indirect benefits of the processing activity covered to the organization, consumers, other stakeholders, and the public

Privacy assessments should be documented and stored for the purposes of providing evidence to regulators if needed. They should also be reviewed periodically and updated any time a processing activity changes. This should be an ongoing part of a company's privacy program and compliance activities.

How organizations should address these requirements

Once a company has determined which state privacy laws are applicable to it, it should review and document its personal data processing activities to determine whether any would likely be considered high risk under the relevant privacy laws.

Once an organization has concluded that it conducts high risk personal data processing activities, it should complete a thorough privacy assessment (considering the requirements of applicable state laws) and work cross-functionally with internal stakeholders to ensure its accuracy and completeness. Key personnel that an organization should collaborate with in drafting privacy assessments include, but are not limited to, legal counsel, privacy officers, security teams, and product managers responsible for data processing activities.

Nixon Peabody's Cybersecurity and Privacy practice can help

Nixon Peabody's Cybersecurity and Privacy attorneys regularly partner with clients on a wide array of compliance initiatives, including in determining privacy law applicability, assessing whether a processing activity is considered high risk, and the conducting and drafting of privacy assessments. Nixon Peabody's Cybersecurity and Privacy attorneys can also recommend safeguards and other measures to ensure the security of your data and thus, your reputation. If you have any questions concerning state privacy law applicability or privacy assessment requirements, please do not hesitate to contact a member of our practice.

For more information on the content of this alert, please contact your Nixon Peabody attorney or:

Jacqueline W. Cooney
617.345.6180
jcooney@nixonpeabody.com

Jenny L. Holmes
585.263.1494
jholmes@nixonpeabody.com

Hannah Edmonds
202.585.8370
hedmonds@nixonpeabody.com