

State Data Privacy Laws Increasingly Require Risk Assessments for High-Risk Processing, 4-30-2026

A growing number of states now require data protection assessments, privacy impact assessments, or risk assessments when certain personal-data processing activities create a heightened risk of harm to consumers.

As of the end of 2025, more than 15 states had enacted comprehensive privacy laws, many of which include data protection assessment requirements, including California, Colorado, Connecticut, Delaware, Florida, Maryland, Minnesota, Montana, Nebraska, New Hampshire, New Jersey, Oregon, Rhode Island, Tennessee, Texas, and Virginia.

These laws generally require covered businesses or controllers to evaluate whether the benefits of a high-risk processing activity outweigh the risks to consumers, consider safeguards, and document the analysis. While the basic concept is similar across states, the trigger for an assessment, the timing, and the scope of required documentation differ from jurisdiction to jurisdiction.

State-by-State Overview

- California - California's regulations require risk assessments for certain high-risk processing activities, such as selling or sharing personal information and processing sensitive personal information. The California Privacy Protection Agency's final regulations include detailed requirements for conducting, documenting, retaining, and submitting risk-assessment information.
- Colorado - Colorado requires controllers to conduct data protection assessments for processing that presents a heightened risk of harm to consumers, including targeted advertising, the sale of personal data, profiling, and the processing of sensitive data. The law further contemplates documentation that evaluates benefits and risks and considers safeguards, and it explicitly allows a single assessment to satisfy multiple state-level obligations where they are substantively similar.
- Connecticut - Connecticut similarly requires assessments for high-risk processing, including targeted advertising, the sale of personal data, profiling that creates a foreseeable risk of harm, and the processing of sensitive data. The Connecticut Data Privacy Act aligns closely with the Colorado-style "heightened risk of harm" model, while giving the state Attorney General broad authority to review and challenge assessment practices.
- Delaware - Delaware's Personal Data Privacy Act requires assessments for covered controllers engaging in high-risk processing activities, including targeted advertising, the sale of personal data, profiling, and the processing of sensitive data. The statute incorporates a risk-based framework and requires written documentation that must be maintained and made available to regulators upon request.
- Florida - Unlike most of the other states listed here, Florida's Digital Bill of Rights is not a broad-based consumer privacy law of general applicability. Instead, it applies primarily to certain large digital-technology companies and, within that narrower scope, requires data protection assessments for specified high-risk processing activities involving personal data.
- Maryland - Maryland requires data protection assessments for processing that presents a heightened risk of harm. The Maryland Online Data Privacy Act follows the general Colorado-style assessment framework and includes additional requirements addressing certain automated decision-making and algorithmic processing activities.
- Minnesota - Minnesota requires assessments for processing activities presenting a heightened risk of harm, including targeted advertising, the sale of personal data, profiling, and the processing of sensitive data. The Minnesota Consumer Data Privacy Act provides a framework for evaluating high-risk processing activities, including documented assessments.
- Montana - Montana's Consumer Data Privacy Act requires data protection assessments for processing that presents a heightened risk of harm, including targeted advertising, the sale of personal data, profiling, and the processing of sensitive data. The law is consistent with the core "heightened risk of harm" trigger seen in many other comprehensive state privacy laws.
- Nebraska - Nebraska requires controllers to conduct and document assessments for targeted advertising, the sale of personal data, profiling that presents a reasonably foreseeable risk of harm, and the processing of sensitive data. The statute also requires consideration of safeguards and mitigation measures for high-risk processing activities.

- New Hampshire – Similarly, New Hampshire requires privacy impact assessments for processing that presents a heightened risk of harm, including targeted advertising, the sale of personal data, the processing of sensitive data, and certain types of profiling.
- New Jersey - New Jersey requires data protection assessments for processing that presents a heightened risk of harm, including targeted advertising, the sale of personal data, profiling, and the processing of sensitive data. The New Jersey Data Privacy Act requires controllers to conduct risk-based data protection assessments that evaluate the benefits of processing against potential risks to consumers, taking into account available safeguards and the context of the processing.
- Oregon - The Oregon Consumer Privacy Act requires data protection assessments for processing that presents a heightened risk of harm, including targeted advertising, the sale of personal data, profiling, and the processing of sensitive data. The statute requires controllers to evaluate the benefits of processing against potential risks to consumers, taking into account the context, purpose, and available safeguards.
- Rhode Island - Rhode Island requires assessments for processing that presents a heightened risk of harm, including targeted advertising, the sale of personal data, certain profiling, and the processing of sensitive data. The Rhode Island Data Transparency and Privacy Protection Act incorporates a “heightened risk” trigger and requires controllers to conduct and maintain data protection assessments for high-risk processing activities.
- Tennessee - Tennessee requires data protection assessments for targeted advertising, the sale of personal data, certain profiling, the processing of sensitive data, and other high-risk activities. The Tennessee Information Protection Act defines high-risk processing to include these categories and requires controllers to document and evaluate such processing.
- Texas - Texas requires data protection assessments for processing that presents a heightened risk of harm, including targeted advertising, the sale of personal data, certain profiling, the processing of sensitive data, and other high-risk activities. The Texas Data Privacy and Security Act reflects the broader state trend toward documented, risk-based privacy governance.
- Virginia - Virginia’s Consumer Data Protection Act requires assessments for processing activities that present a heightened risk of harm, including targeted advertising, the sale of personal data, profiling, and the processing of sensitive data. Virginia was one of the first states to adopt a robust assessment framework, and its statute has served as a model for many subsequently enacted laws.

Practical Implications

For multi-state businesses, the biggest compliance challenge is harmonizing different triggers, retention rules, and legal-review standards into a single assessment process. Several states also permit a single assessment to satisfy comparable requirements elsewhere, which can reduce duplication if a company uses a consistent methodology.

Companies should inventory processing activities, map the states whose laws apply, and build a repeatable review process for high-risk uses of personal data. In practice, that means identifying the processing purpose, the categories of data involved, the potential risk of consumer harm, and the safeguards designed to mitigate that risk.

Conclusion

With more than 15 state privacy laws now imposing assessment-related obligations, businesses should treat privacy assessments as a core governance tool rather than an after-the-fact compliance exercise. Organizations that process personal data at scale should confirm which state laws apply, update internal workflows, and preserve assessment records in anticipation of regulatory scrutiny.

Authors:

Richard J. Perr
 Co-Managing Partner of Philadelphia Office,
 Co-Chair of Financial Services & Institutions Practice Group

Monica M. Littman
 Partner

Graeme Hogan
 Partner

Shera Anderson
Of Counsel

Dominic Borelli
Attorney

Kristen Ruotolo
Attorney

Samuel Sjosten
Attorney