Cooley

Small State, Big Bite: What Sets Vermont's New Privacy Law Apart

June 30, 2026

Vermont became the 23rd state to enact a comprehensive consumer privacy law with the Vermont Data Privacy and Online Surveillance Act (VDPOSA), which was signed into law on June 16, 2026. At a high level, the VDPOSA takes the now-familiar US state law approach of a controller/processor framework with consumer rights. But it also includes a number of more expansive and distinctive provisions – such as low applicability thresholds for sensitive data and stand-alone provisions for consumer health data – that put it alongside Connecticut at the more aggressive end of the state consumer privacy law spectrum. As a result, despite Vermont's small size, companies may need to reevaluate and update their multistate privacy compliance programs to account for these new requirements from the Green Mountain State.

Below, we describe key features of the VDPOSA and what companies should do to evaluate and update their compliance status before the law takes effect on January 1, 2028.

Low applicability thresholds

The VDPOSA's general applicability thresholds encompass companies that:

1. Control or process personal data for at least 35,000 Vermont residents.
2. Control or process sensitive data for at least 3,000 Vermont residents.
3. Offer for sale in trade or commerce personal data of at least 3,000 Vermont residents.

The regular personal data threshold of 35,000 residents is not particularly low relative to Vermont's population. However, the VDPOSA's thresholds for sensitive data and sales of personal data are more aggressive than similar laws in most other states. Vermont does not go as far as Connecticut, whose similar thresholds are triggered by processing any amount of sensitive data or selling any amount of personal data, but its thresholds of 3,000 are still quite low. As a result, they could easily ensnare companies that are handling sensitive data or selling personal data at any sort of scale, particularly given the law's broad definitions of "sensitive data" and "sale."

Consumer health data

The VDPOSA also includes consumer health data protections that only a few other states – such as Connecticut via its consumer privacy law, Washington via its stand-alone My Health My Data Act and Nevada's similar law – have enacted laws to protect. Companies that handle any amount of consumer health data must meet the law's provisions related to such data, regardless of whether they meet the general VDPOSA thresholds discussed above.

The law's requirements for consumer health data include requiring an affirmative opt-in consent before selling, or offering to sell, consumer health data and prohibiting geo-fencing within 1,850 feet of any healthcare facility (for the purpose of identifying, tracking, collecting data from or sending any notification to consumers regarding their health data). The VDPOSA also requires a company's employees and contractors to be subject to a contractual or statutory duty of confidentiality before accessing consumer health data. Companies processing consumer health data must ensure that they comply with these requirements, which may also require updating existing applicable contracts to include a contractual duty of confidentiality.

Due to the VDPOSA's broad definition of consumer health data, and the relevant obligations being triggered if a company handles any amount of consumer health data, companies could easily become subject to these requirements, even if they do not think of themselves as a healthcare-related business.

Expansion of sensitive data and additional obligations

As referenced above, the VDPOSA's definition of sensitive data is, like Connecticut's, one of the broadest among the 23 state consumer privacy laws. For example, Vermont includes financial account numbers with login credentials and certain government-issued identification numbers as sensitive data. Vermont also – similar to California, Colorado and Connecticut – treats neural data as a type of sensitive data, albeit limiting it only to data generated by the central nervous system, instead of both the central and peripheral nervous systems. Vermont also follows recent privacy laws' trend of explicitly including nonbinary or transgender status as sensitive data.

In addition to the VDPOSA being triggered by a company's control or processing of sensitive data of only 3,000 Vermont residents, handling such sensitive data triggers heightened obligations, including a requirement to obtain affirmative opt-in consent from consumers before processing their sensitive data. Additionally, Vermont requires companies to only process data that is necessary in relation to the purpose they disclose to consumers when they collect their data, and to obtain opt-in consent from consumers before selling any sensitive data.

Companies should assess their sensitive data collection and disclosure practices to ensure that their handling of data elements treated as sensitive data in Vermont complies with the VDPOSA.

Transparency about AI training

Reflecting recent regulatory and legislative concerns about AI, Vermont, like Connecticut, imposes a transparency obligation on companies regarding large language models (LLMs). Companies must include, in their privacy notice, a statement disclosing whether they collect, use or sell personal data for the purpose of training LLMs. For the many companies that leverage personal data in training their AI models, or sell personal data to train LLMs, this obligation will likely require updates to their current privacy disclosures and could generate additional consumer friction.

Broadening the right to access

Vermont has followed the lead of Connecticut and Minnesota in expanding a consumer's right to access information about a company's handling of their personal data. Under the VDPOSA, a consumer can obtain a list of third parties to which the company has sold the particular consumer's personal data – or, if the company does not maintain this list, it must instead provide the consumer with a list of all third parties to which the company sells personal data of consumers generally. Even if companies take the latter, less granular approach that is not specific to the particular consumer making the access request, for many companies preparing to honor such requests is likely to require nontrivial back-end data mapping and other compliance work.

Derived data

Data derived from other information about a consumer is commonly understood to be personal data. However, the VDPOSA goes a step further by including derived data as a stand-alone defined term and explicitly including it as a type of personal data.

Enforcement and cure period

The VDPOSA does not contain a private right of action, so like most other state consumer privacy laws, it will be enforced exclusively by the state attorney general. Similar to some other state laws, Vermont also includes a 60-day cure period for a limited time following the law's initial rollout – between January 1, 2028, and June 30, 2029 – to help businesses ease into compliance with the VDPOSA.

Interestingly, Vermont's legislators also included a statement that if additional resources are not provided to the Office of the Attorney General to enforce the VDPOSA, then the General Assembly may consider adding a private right of action. This statement is unique among state consumer privacy laws, and the addition of a private right of action would represent a seismic shift in enforcement and potential exposure for companies. However, it appears unlikely that such a private right of action will make it into law in Vermont, as it would undoubtedly face

vociferous opposition from industry.

What should companies do?

Due to Vermont's relatively aggressive and distinctive provisions for certain types of personal data and activities, companies should work closely with privacy counsel to assess potential exposure under the VDPOSA, as well as similar provisions under Connecticut's amended consumer privacy law. Relevant steps should include:

1. **Assess whether you are in scope of the VDPOSA.** Vermont's relatively low and distinctive thresholds for certain activities – such as selling personal data or handling sensitive data or consumer health data – will bring many companies within scope of the law. Companies should carefully assess whether they are engaging in such activities, particularly given the broad ways that terms like "sensitive data," "consumer health data" and "sale" are defined under the VDPOSA.
2. **Revisit your sensitive data and consumer health data practices and obligations.** Vermont includes many additional data elements as sensitive data and expands companies' obligations for handling of sensitive data. It also has separate obligations that trigger if a company handles any amount of consumer health data (which is also defined as a type of sensitive data). These obligations related to specific data types may require additional compliance efforts.
3. **Update privacy notices.** Vermont requires companies to disclose in their privacy notice whether any personal data is collected, used or sold for training LLMs. Companies should also review their privacy notice for other updates needed to address the VDPOSA, such as whether their disclosures about their handling of sensitive data are accurate under the VDPOSA's broad definition of that term.
4. **Track data flows for sales of personal data.** Under the VDPOSA, consumers have the right to obtain a list of all third parties to which their personal data is sold, so companies should conduct internal data mapping and similar exercises to ensure that they can fulfill this obligation. Companies also need to understand their personal data sales to assess whether they meet the VDPOSA's applicability thresholds, one of which triggers if a company sells personal data of at least 3,000 Vermont residents.

Key Contacts

Kristen Mathews **New York**	**kmathews@cooley.com**
Christopher Suhler Colorado	csuhler@cooley.com +1 720 566 4376