Compliance Guidance for the New Vermont Data Privacy and Online Surveillance Act (VDPOSA)

Vermont Becomes the 23rd US State to Enact a Consumer Privacy Law

Privacy, Cyber & AI Decoded Alert | 4 min read
Jul 27, 2026

By: Jason J. Oliveri

On June 16, 2026, Governor Scott signed S.71, the Vermont Data Privacy and Online Surveillance Act (VDPOSA), making Vermont the 23rd state to enact a comprehensive consumer privacy law.

While the final bill is more business-friendly than its predecessor—most notably, the controversial private right of action was stripped out—the VDPOSA imposes several obligations that go beyond the typical Connecticut-style framework, and companies should not mistake the **January 1, 2028,** effective date for breathing room.

Our following alert summarizes the scope of the new law, the provisions that materially differ the most from the multi-state baseline, and the compliance planning steps businesses should begin taking now.

Scope and Applicability

What's New?

- The VDPOSA adopts one of the lowest applicability thresholds in the country, closely tracking the 2025 version of the Connecticut Data Privacy Act.
- The law will be enforced exclusively by the Vermont Attorney General, with civil penalties of up to $10,000 per violation.

What is Required?

The VDPOSA applies to any person or entity that conducts business in Vermont, or that produces products or services targeted to Vermont residents, and that during the preceding calendar year (excluding data processed solely to complete a payment transaction) either:

- controlled or processed the personal data of at least 35,000 consumers;
- controlled or processed the sensitive personal data of at least 3,000 consumers; or
- offered for sale the personal data of at least 3,000 consumers.

Enforcement discretion is tempered by a 60-day cure period running from **January 1, 2028, through June 30, 2029,** after which the right to cure sunsets. Businesses should treat the cure window as a planning phase, not a safety net.

Consumer Rights

What's New?

Vermont provides consumers with the now familiar suite of data subject rights, but with several important expansions that will require operational tuning.

What is Required?

Controllers must honor the following rights, generally responding within 45 days of receipt (with a 60-day appeal decision window):

- **Access and confirmation,** including whether the controller is using profiling to make legally or similarly significant decisions.
- **Correction, deletion, and portability of personal data.**
- **Opt-out of targeted advertising, the sale of personal data, and profiling** in furtherance of solely automated decisions producing legal or similarly significant effects.
- **Third-party disclosure list.**
  - Consumers have the right to obtain a list of specific third parties to which their personal data has been disclosed. Or, if the controller does not maintain that data on a per-consumer basis, a disclosure list of all third parties to which personal data has been disclosed must be provided.
- **Human review and appeal of profiling.**

    - Consumers whose data was profiled in furtherance of a decision producing a legal or similarly significant effect may question the outcome, be informed of the reasoning, and review the data used. For housing decisions, consumers also have the right to correct inaccurate data and have the decision reevaluated.

- **Restricted access response categories.**

    - Unlike most state laws, the VDPOSA prohibits controllers from disclosing (and instead requires controllers only to confirm the existence of) certain data categories in response to access requests, including Social Security numbers, government-issued ID numbers, financial account numbers, health insurance and medical identification numbers, passwords and security questions, and biometric data.

Consumers may also designate an authorized agent to exercise opt-out rights (including for profiling) and may transmit an opt-out preference signal to opt out of the sale of personal data or targeted advertising.

Sensitive Data and Consumer Health Data

What's New?

Vermont's definition of "sensitive data" is one of the broadest in the country, and consumer health data protections apply without a threshold—meaning even businesses outside the general scope of the law may be subject to them.

What is Required?

- **The expansive "sensitive data" definition includes data revealing:**

    - racial or ethnic origin, religious beliefs, sex life, sexual orientation, nonbinary or transgender status, citizenship or immigration status, or a mental or physical health condition, diagnosis, disability, or treatment;

    - consumer health data (separately defined to capture gender affirming health data and reproductive or sexual health data);

    - genetic and biometric data;

    - data collected from an individual known to be a child; precise geolocation data; neural data;

    - financial account credentials; and

    - government issued identification numbers.

  - Processing sensitive data generally requires consumer consent, and the sale of sensitive data likewise requires consent.
- **No threshold for consumer health data.**
  - The consumer health data restrictions apply to any person conducting business in Vermont or targeting Vermont residents, regardless of the general applicability thresholds. Covered persons:
    - may not give employees or contractors access to consumer health data unless those individuals are bound by a contractual or statutory duty of confidentiality;
    - may not provide processor access absent a compliant processor contract;
    - may not use a geofence to establish a virtual boundary within 1,850 feet of any healthcare facility—including any mental health facility or reproductive or sexual health facility—for purposes of identifying, tracking, collecting data from, or sending notifications to a consumer regarding the consumer's health data; and
    - may not sell or offer to sell consumer health data without first obtaining the consumer's consent.

Data Protection and Profiling Assessments

What's New?

Vermont goes further than most states by requiring a separate impact assessment for any profiling used to make legally or similarly significant decisions, layered on top of the more familiar data protection assessment requirement.

What is Required?

Controllers must conduct and document data protection assessments for processing activities presenting a heightened risk of harm, including:

1. processing for targeted advertising;
2. the sale of personal data;
3. profiling that presents a reasonably foreseeable risk of unfair treatment, financial or reputational injury, intrusion on privacy, or other substantial injury; and
4. the processing of sensitive data.

A separate profiling impact assessment is required for any profiling used to make decisions producing legal or similarly significant effects, with prescribed components including purpose disclosure and the categories of a minor's personal data possessed by the online product, service, or feature.

Assessments are confidential but may be requested by the Attorney General.

AI Training Disclosure

What's New?

Vermont is only the second state—after Connecticut—to require businesses to disclose AI training practices in their privacy notices.

What is Required?

The privacy notice a controller provides to consumers must state whether the controller collects, uses, or sells personal data for the purpose of training large language models.

The provision should be read alongside Connecticut's amended privacy law, which took effect July 1, 2026, and reflects a growing state legislative focus on AI transparency.

Protections for Minors

What's New?

The VDPOSA supplements Vermont's Age Appropriate Design Code Act (S.69/Act 63, signed the same day) by imposing specific restrictions on the processing of teenagers' data.

What is Required?

- Where a controller has actual knowledge, and willfully disregards, that a consumer is at least 13 but younger than 18 years of age, the controller may not process that consumer's personal data for targeted advertising and may not sell that consumer's personal data.
- The combined "actual knowledge and willful disregard" formulation is worth flagging for businesses accustomed to a pure "actual knowledge" standard, as it may affect how teenage signals are evaluated. Companies already complying with Connecticut's teen-focused restrictions will find the substantive prohibition familiar, but should confirm that their age signaling and knowledge attribution controls extend to Vermont operations.

Companion Legislation: Data Broker Reforms (H.211)

Governor Scott signed House Bill 211 on the same day as the VDPOSA. Its data broker and edtech provisions take effect **January 1, 2027,** and require, among other things:

- annual data broker registration with the Vermont Secretary of State and payment of a $900 registration fee;
- accelerated 30-day registration once a data broker first meets the statutory definition;
- expanded mandatory disclosures, including whether the broker collects precise geolocation data or immigration status; whether it has sold or shared consumer data with foreign actors, government entities, or "developer[s] of a GenAI system or model;" and the URL of a page addressing consumer rights;
- a new $20,000 bond requirement; and
- data broker-specific security breach notice requirements.

Data brokers and companies whose vendor arrangements may implicate the definition should reassess their Vermont posture well before the 2027 effective date.

Compliance Planning Steps

The January 1, 2028, effective date is deceptive. Because the VDPOSA layers Connecticut-style obligations onto several Vermont-specific enhancements—and since the data broker and Age Appropriate Design Code obligations arrive sooner—businesses subject to the VDPOSA should begin the following compliance activities now:

1. Reassess applicability against the 35,000/3,000/3,000 thresholds and inventory Vermont resident data flows.
2. Update sensitive data inventories to capture neural data, gender affirming health data, and reproductive or sexual health data, and confirm opt-in consent workflows.
3. Evaluate consumer health data practices, including employee confidentiality obligations, geofencing controls near healthcare facilities, and any sale of consumer health data, regardless of whether the general law applies.
4. Refresh privacy notices to include AI training disclosures and to align with Connecticut's amended notice standard.
5. Design a profiling impact assessment framework distinct from your existing data protection assessment template, and confirm assessments will be preserved as confidential and producible upon Attorney General request.
6. Refine data subject rights processes to accommodate the third-party disclosure list, human review, and appeal of profiling (including housing-specific correction and reevaluation), and the restricted response categories that must not be disclosed in access responses.

7. Configure teen data controls for consumers between 13 and 17 years old where the controller has actual knowledge of age.
8. For data brokers, prepare for the January 1, 2027, registration, bond, disclosure, and breach notice obligations under H.211.

We Are Here to Help

Companies with mature Connecticut Data Privacy Act programs will find the VDPOSA less burdensome to comply with. However, the Vermont-specific overlays—particularly around consumer health data, profiling assessments, restricted access responses, and AI training disclosures—will require targeted work.

Hinshaw's Data Privacy, AI & Cybersecurity team is available to help clients scope Vermont's requirements against their existing multi-state compliance frameworks.

Hinshaw & Culbertson LLP is a U.S.-based law firm with offices nationwide. The firm's national reputation spans the insurance industry, the financial services sector, professional services, and other highly regulated industries. Hinshaw provides holistic legal solutions—from litigation and dispute resolution, and business advisory and transactional services, to regulatory compliance—for clients of all sizes. Visit www.hinshawlaw.com for more information and follow @Hinshaw on LinkedIn and X.

Related People

Jason J. Oliveri

Partner

212-471-6237

Related Capabilities

Corporate & Transactions

Data Privacy, AI & Cybersecurity

Healthcare

Regulatory & Compliance

Website Data Privacy

Related Insights

AI Governance Expectations on the Rise for Insurers Amid New Regulatory Activity

Jason Oliveri Unpacks Cybersecurity and Healthcare Compliance Risks With AI Agents