



VERMONT DATA PRIVACY AND ONLINE SURVEILLANCE ACT (VDPOSA)

CHECKLIST



USERCENTRICS

Vermont Data Privacy and Online Surveillance Act (VDPOSA) gives Vermont residents rights over how their personal data is collected and used.

This checklist walks through steps that support your compliance efforts under the Act, along with recommended best practices for privacy-related user experience.



Important to know:

Action	Date
Effective date	January 1, 2028
Cure period	60 days' notice, available through June 30, 2029; discretionary after that
Retroactive	No

Note: This is a separate statute from Vermont's Age-Appropriate Design Code (the "Vermont Kids Code"), which has an earlier effective date (January 1, 2027) and a different scope.

1 Determine If Your Company Is Required to Comply

If your organization conducts business in Vermont or targets Vermont residents, and during the preceding calendar year met at least one of the following:

- Controlled or processed the personal data of 35,000 or more consumers (excluding data processed solely for payment transactions)
- Controlled or processed sensitive data of 3,000 or more consumers
- Offered for sale the personal data of 3,000 or more consumers

There is no revenue threshold. Consumer health data provisions apply to any business regardless of scale, with no threshold at all.

Exempt entities:

- Federal, state, tribal, and local government entities and instrumentalities, acting in the ordinary course of operation
- [HIPAA](#)-covered entities and business associates (excluding a hybrid entity's non-health-care components)
- State- or federally chartered banks and credit unions, and their affiliates/subsidiaries principally engaged in financial activities
- Insurance entities regulated under Vermont law
- Agents, broker-dealers, investment advisers, and investment adviser representatives regulated by Vermont's Department of Financial Regulation or the SEC
- Third-party administrators regulated by Vermont's Department of Financial Regulation
- Health care providers and facilities maintaining protected health information in accordance with Vermont law and HIPAA
- Victim services organizations collecting data on victims or witnesses of abuse, violence, or stalking
- Nonprofit organizations established to detect and prevent insurance fraud, or providing enrollment-verification data reporting for postsecondary schools
- FCC-licensed radio or television stations, and nonprofits that provide programming to radio or television networks

Data-level exemptions:

- Protected health information under HIPAA
- Patient-identifying information under 42 U.S.C. (substance-use research/treatment data)
- [FCRA](#) data
- FERPA data
- [GLBA](#) data
- Driver's Privacy Protection Act data
- Farm Credit Act data
- Controlled Substances Act data
- Payment transaction data
- Employee, contractor, and business contact data processed in an employment context
- Emergency contact/notification information

2 Create a Comprehensive Privacy Policy

Businesses are required to disclose:

- Categories of personal data processed
- Purposes for processing
- Categories of third parties data is sold to, if any
- Targeted advertising disclosures
- Whether personal data is used to train large language models (LLMs)
- A contact mechanism
- The date of last update

3 Inform Consumers About Their Rights

Consumers' rights under the VDPOSA:

- **Right of access:** Confirm processing and access personal data, including whether it's used in profiling for legally significant decisions
- **Right of correction:** Fix outdated or inaccurate information
- **Right of deletion:** Of data provided by or obtained about them
- **Right of portability:** In a machine-readable format where processing is automated
- **Right to opt out:** Of targeted advertising, sale of personal data, and profiling used in legally significant automated decisions
- **Right to challenge profiling:** Question a legal or significant decision resulting from profiling, review the data used, and, for housing decisions specifically, request correction and re-evaluation
- **Right to the third-party sales list:** Obtain a list of third parties their data was sold to

4 Disclose Whether Personal Data Is Used to Train Large Language Models

Vermont's privacy notice must state whether the business collects, uses, or sells personal data to train large language models. This is a requirement it shares with only Connecticut to date.

5 Honor Opt-Out Preference Signals

Vermont requires businesses to honor browser- or platform-level opt-out signals for targeted advertising and data sales. The signal must reflect an affirmative consumer choice with no default enabled, be consumer-friendly, align with other applicable mechanisms where possible, and allow the business to verify Vermont residency.

6 Obtain Affirmative Consent for Sensitive Personal Data

[Sensitive data](#) under the VDPOSA is defined broadly, and includes:

- Racial or ethnic origin
- Religious beliefs
- Sex life or sexual orientation
- Transgender or nonbinary status
- Citizenship or immigration status

- Mental or physical health condition, diagnosis, disability, or treatment
- Consumer health data
- Genetic or biometric data
- Personal data of known children
- Precise geolocation (within a 1,750-foot radius)
- Neural data
- Financial account credentials
- Certain government-issued ID numbers

7 Apply Enhanced Protections to Consumer Health Data

These provisions apply regardless of size or thresholds. Obtain consent before selling consumer health data, hold employees who access it to a duty of confidentiality, and do not deploy a geofence within 1,850 feet of a health care, mental health, or reproductive or sexual health facility.

8 Restrict Targeted Advertising and Data Sale Involving Minors Ages 13–17

Where your business has actual knowledge, or willfully disregards, that a consumer is between 13 and 17, restrict targeted advertising and sale of their data accordingly. Vermont's separate Age-Appropriate Design Code also applies to this age group. [COPPA](#) governs consumers under 13.

9 Provide a Consent Revocation Mechanism

Revocation must be as easy as the method used to grant consent. Cease the relevant processing within 15 days of a revocation request.

10 Audit Consent Interfaces for Dark Patterns

Consent obtained through a [dark pattern](#) is invalid. This includes any interface designed to subvert or impair a consumer's autonomy or choice.

11 Notify Consumers of Material Privacy Notice Changes

Where a change would result in materially different processing of previously collected data, notify consumers and give them the opportunity to withdraw consent before that processing occurs. A [Privacy Policy Generator](#) and your [CMP](#) can help.

12 Enable Consumers to Make Data Subject Access Requests (DSARs)

Respond within 45 days from the date the [DSAR](#) is received, extendable by an additional 45 days if the business notifies the consumer of the extension and its reason within that first 45-day window. Appeals must be resolved within 60 days. If denied, the consumer may escalate to the Vermont Attorney General.

13 Conduct Data Protection Assessments and Profiling Impact Assessments

Required for targeted advertising, data sales, higher-risk profiling, and sensitive data processing. Profiling impact assessments specifically must cover purpose, risk analysis, mitigation, data categories, and post-deployment monitoring.

Falling thresholds, rising enforcement and litigation, eroding ad revenue. Do you know your risk?

GET IN TOUCH