



VIRGINIA CONSUMER DATA PROTECTION ACT (VCDPA)

CHECKLIST



 **USERCENTRICS**

Virginia Consumer Data Protection Act (VCDPA) gives Virginia 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, 2023
Retroactive	No
Known-child protections (SB 361/HB 707)	Effective January 1, 2025
Geolocation data sale ban (SB 338)	Effective July 1, 2026

Note: A separate Virginia statute, the Reproductive Health Data law (SB 754, effective July 1, 2025), imposes its own protections beyond VCDPA thresholds, including a private right of action and treble damages.

1 Determine If Your Company Is Required to Comply

If your for-profit organization:

- Processes the personal data of at least 100,000 Virginia consumers, or
- Processes the personal data of at least 25,000 Virginia consumers, and derives at least 50 percent of annual revenue from selling personal data

Entity-level exemptions:

- Bodies, authorities, boards, bureaus, commissions, districts, or agencies of the Commonwealth or of any political subdivision
- [GLBA](#)-regulated financial institutions and their data

- [HIPAA](#)/HITECH-covered entities and business associates
- Nonprofit organizations
- Institutions of higher education

Data-level exemptions:

- Protected health information under HIPAA
- [FCRA](#)-regulated data
- Driver's Privacy Protection Act data
- Farm Credit Act data
- FERPA-regulated data
- [COPPA](#)-regulated data
- Identifiable private information for human-subjects research under 45 C.F.R.
- Employee and job applicant data processed within the context of that role
- Emergency contact information
- Data necessary to administer benefits for another individual
- Publicly available information

2 Create a Comprehensive Privacy Policy

Businesses are required to inform consumers at or before the point of data collection:

- Categories of personal data processed
- Purposes for which data is processed
- Categories of personal data the controller shares with third parties, if any
- Categories of third parties the controller shares personal data with, if any

Rights: Inform website visitors of their privacy rights and how to exercise them, including how a consumer may appeal a controller's decision.

Language: Keep the [privacy policy](#) clear and easy to understand.

Implementation: As a best practice, pair the privacy notice with an opt-out mechanism. For example, use a banner or popup when visitors visit your site, [powered by a CMP](#).

3 Inform Consumers About Their Rights

Consumers' rights under the VCDPA:

- **Right to know:** Whether personal data is processed, with confirmation and access to it
- **Right to access:** Request and receive a copy of their personal data
- **Right to correction:** Updates or corrections to inaccuracies in personal data collected
- **Right to deletion:** Personal data collected about them (with exceptions)

- **Right to data portability:** A copy of personal data in a portable, readily usable format
- **Right to opt out:** Of processing for the purposes of sale, targeted advertising, or profiling for decisions with legal or similarly significant effects
- **Right to non-discrimination:** For exercising privacy rights
- **Right of minors:** Consent must be obtained from a parent/guardian before a known child's (under 13) personal data is collected
- **Right to restrict use of sensitive personal information:** Limit or refuse collection or use of personal data the law classifies as sensitive

4 Apply Enhanced Protections for Known Children Under 13

Under SB 361/HB 707, obtain parental consent before:

- Processing a known child's personal data for targeted advertising, sale, or profiling
- Collecting a known child's precise geolocation data (absent a necessity exception with an active collection-indicator signal)

5 As a Best Practice, Review and Update Your Privacy Policy or Notice Every 12 Months

Review operations and potential legal changes every 12 months. Update the Privacy Policy and its effective date, even if no other changes are made.

Transparency: Keep the information visitors must be notified about clear, comprehensive, and up to date, with the last-update date clearly visible. A [Privacy Policy Generator](#) can help.

Data sold: List all categories of personal information your business has sold in the past 12 months.

6 Enable Clear Options When Consent Is Required

When: If the personal data collected is sensitive, or that of a child.

Availability: Easily accessible on your website.

Method: Via a CMP.

7 Authenticate Consent or Opt-Out for Collection of Sensitive Personal Data or Data From Minors

Sensitive personal data: Consent is required for processing of [sensitive personal data](#).

Consent for children: Obtain consent from a parent or legal guardian for collection of personal data if the data subject is 13 or younger.

8 Do Not Sell Precise Geolocation Data

Effective July 1, 2026 (SB 338), controllers may not sell consumers' precise geolocation data. Precise geolocation data is defined as information identifying a person's location within a 1,750-foot radius.

9 Enable and Respond to Data Subject Access Requests (DSARs)

Provide one or more contact options (e.g., toll-free phone number, web form, email). Set up a system to enable submission, verification, and tracking of [DSARs](#). If identity cannot reasonably be verified, inform the consumer and explain why, and enable them to rectify. Keep records of all requests and responses for two years.

Respond within 45 days from the date the request 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.

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

GET IN TOUCH