

Virginia Data Collection Audit

Accessible text alternative to the on-screen accordion (expand/collapse) interaction. This document presents the same five compliance categories and content in a linear, screen-reader- and keyboard-navigable format, matching WCAG 2.1 AA / Section 508 requirements.

Instructions as presented on-screen: Select each category below to review the operational compliance rules under the VCDPA. Select each tab to learn more.

1. Data Minimization Standards

Compliant State

Limit all personal data collection to what is strictly adequate, relevant, and reasonably necessary for the business purposes you explicitly disclosed to the consumer.

Before adding a new data field to an online application form or an AI tool prompt, verify its direct business function. For example, capturing a customer's name and email to deliver a retail digital receipt is legally compliant. Capturing extreme, unnecessary data points—like a Social Security Number—for a standard loyalty account represents a massive data over-collection violation under Virginia law.

Image description (alt text): Illustration of a funnel labeled “Data Minimization Standards: Limit Collection & Retention, Virginia VCDPA Compliant,” showing a wide stream of data icons narrowing down to a small set of “selected data” icons at the bottom, alongside a gavel.

2. Right to Delete Processing

Consumer Right

Virginia residents have the strict legal right to request the complete deletion of any personal data an organization has obtained about them.

When a resident submits an authenticated deletion request, the data must be permanently purged from active organizational databases, backup archives, and modern generative AI training pipelines. Organizations must establish clear, easily accessible contact methods (such as a secure web form) allowing consumers to invoke these requests without requiring them to build a new account.

Image description (alt text): Illustration labeled “Right to Delete Processing: Enforced Erase, Virginia VCDPA Compliant,” showing a gavel connected to icons for databases, cloud storage, and devices, all pointing toward a recycling bin labeled “Data.”

3. Profiling & AI Automated Decisions

Mandatory Oversight

Consumers have the right to opt out of automated data processing and “profiling” used to make high-stakes decisions that yield legal or similarly significant life impacts.

If your organization utilizes automated algorithms or AI scoring tools to evaluate individuals for credit approvals, housing access, employment hiring suitability, or insurance rates, you must implement human oversight. The system must allow users to opt out of the purely automated path, routing their files to a live human review panel to prevent biased or discriminatory algorithmic outcomes.

Image description (alt text): Illustration labeled “Profiling & AI Automated Decisions: Opt-Out Rights Enforced, Virginia VCDPA Compliant,” showing a gavel connected to a network of icons representing people and automated scoring/review processes.

4. Sensitive Data Guardrails

Prior Opt-In Required

Unlike standard personal information, organizations are strictly prohibited from processing “Sensitive Data” without obtaining explicit, affirmative, prior opt-in consent from the consumer.

Under the VCDPA, sensitive data includes a consumer's racial or ethnic origin, religious beliefs, mental/physical health diagnoses, sexual orientation, citizenship status, precise geolocation data, or the personal information of a known child under 13. To process this info legally, you must present a clear, un-checked checkbox or prompt before collection begins. Sneaking this tracking into fine-print terms or using deceptive user interfaces (Dark Patterns) is entirely illegal.

Image description (alt text): Illustration labeled “Sensitive Data Guardrails: Opt-In Required, Virginia VCDPA Compliant,” showing a gavel connected to an open vault or safe icon representing protected sensitive data.

5. Reproductive Health Guardrails

Explicit Opt-In Consent Required for Health, Tracking, or Clinic Location Data

- The Law: Virginia Senate Bill 754.
- The Rule: Explicit opt-in consent required.
- Data Covered: Reproductive/sexual health tracking, pregnancy, and birth control records.
- Location Rules: No tracking device location near health clinics.
- Legal Risk: Enforceable via a private right of action.

Image description (alt text): Illustration labeled “Reproductive Health Guardrails: Opt-In Consent Required, Virginia VCDPA Compliant,” showing a gavel connected to a medical cross icon with a DNA strand, representing reproductive health data.

Educational Use Only. Not Legal Advice. Consult with qualified legal counsel for specific VCDPA compliance requirements.