PRIVACY POLICY

Effective Date: July 15, 2026

Vantage Verify ("Company," "we," "us," or "our") is committed to protecting the privacy and security of the personal and sensitive information we collect. This Privacy Policy outlines our practices regarding the collection, use, disclosure, and protection of information obtained through our website (http://www.vantageverify.org), our mobile testing services, and our comprehensive compliance offerings.

1. INFORMATION WE COLLECT

In the course of providing mobile drug testing, alcohol testing, I-9 verification, DNA collection, background checks, notary, and fingerprinting services, we may collect the following categories of information (depending on the services requested and applicable law):

- **Personal Identifiers:** Name, date of birth, Social Security number (SSN), government-issued identification numbers (e.g., driver's license number, passport number), signature, and other identifiers necessary to verify identity and fulfill service requirements.
- **Contact Information:** Physical address, mailing/billing address, email address, and telephone number.
- **Employment and Eligibility Information:** Employer name, worksite/location, job title/position, employee or applicant status, employment history and authorization details relevant to background screening and I-9 verification, and other information supplied by an employer or authorized requester.
- **Testing and Health-Related Information (as applicable):** Collection details (date/time, collector identity), test authorization forms, drug and alcohol test results and related documentation (including confirmatory testing), breath alcohol levels, and related compliance records.
- **DNA-Related Information (as applicable):** DNA specimen collection information and associated identifiers and documentation required for lawful processing.
- **Biometric Information:** Fingerprints and fingerprint-derived templates or identifiers used for verification and background check submissions (as applicable).
- **Background Check Information (as applicable):** Information needed to request background checks and information returned from background screening sources (e.g., identity verification outputs, records or reports provided by authorized providers), subject to applicable law and permissible purpose.
- **Notary-Related Information (as applicable):** Identity verification details required by law for notarial acts, transaction details recorded in a notary journal where required/maintained, and copies of documents only where permitted or required by law and/or requested by the customer.
- **Technical and Usage Information (Website/Online Services):** IP address, device identifiers, browser type, operating system, referring/exit pages, and usage data collected through cookies, pixels, analytics tools, or similar technologies.

- **Communications:** Information you provide when you contact us, schedule services, submit forms, or communicate with us (e.g., email content, call metadata, and appointment notes).

We do not intentionally collect information from children under 13. If you believe a child has provided us information, please contact us so we can address it appropriately.

2. HOW WE COLLECT INFORMATION

We collect information in the following ways:

- **Directly From You:** When you schedule services, complete consent or authorization forms, present identification, submit to testing, provide fingerprints, request notary services, communicate with us, or otherwise interact with our staff.
- **From Employers/Authorized Requesters:** When an employer, contracting entity, or other authorized requester provides information necessary to initiate services (e.g., identity and employment details, testing authorization, scheduling details).
- **From Laboratories, MROs, and Background Check Providers:** When we receive confirmed results, verifications, or reports from certified laboratories, Medical Review Officers (MROs), fingerprint submission channels, and background screening vendors, as applicable.
- **Automatically Through Our Website:** Through cookies and similar technologies when you visit or use our website (see Section 8: Cookies & Website Tracking).
- **From Government/Regulatory Sources:** Where permitted or required, including verification systems or reporting channels used for compliance.

3. HOW WE USE YOUR INFORMATION

Vantage Verify uses the collected information for professional and operational purposes, including:

- **Service Delivery:** To perform on-site drug and alcohol testing, DNA collection, fingerprinting, notary services, I-9 verification, and related scheduling and logistics.
- **Verification and Identity Confirmation:** To confirm identity before providing services and to prevent fraud.
- **Compliance, Reporting, and Recordkeeping:** To comply with applicable laws and regulations, including DOT requirements when applicable, and to maintain legally defensible records and chain-of-custody documentation.
- **Results Processing:** To transmit specimens to laboratories, obtain results, work with MROs as required, and deliver results to authorized parties.
- **Background Screening:** To initiate and manage background checks and related verification steps as requested by authorized parties and as permitted by law.
- **Customer Support and Communications:** To respond to inquiries, provide service updates, deliver notices, and communicate about appointments and operational issues.
- **Billing and Administrative Purposes:** To process payments (where applicable), maintain accounts, and manage our business operations.

- **Security, Auditing, and Quality Assurance:** To protect our personnel, customers, and testing candidates, to investigate incidents, to enforce our policies, and to improve service quality.
- **Legal Purposes:** To establish, exercise, or defend legal claims; comply with subpoenas, court orders, and lawful requests; and prevent or address suspected wrongdoing.

We do not use sensitive information for purposes not permitted by law and do not sell personal information.

4. DISCLOSURE OF INFORMATION

We do not sell personal information. We disclose information only as necessary to provide services, comply with law, and operate our business, including:

- **Authorized Employers and Contracting Entities:** Where testing, I-9 verification, background checks, or other services are requested by an employer or contracting entity, we may provide results and related documentation (including chain-of-custody records) to the designated HR, safety, compliance, or operations representatives, consistent with authorizations and applicable law.
- **Accredited Laboratories, MROs, and Clinical Partners:** Specimens and related information are provided to certified laboratories and Medical Review Officers (MROs) (or other appropriate professionals) for analysis, verification, and reporting, as applicable.
- **Background Check, Fingerprinting, and Identity Verification Providers:** We may share identifiers and required information with vendors and channels used to submit fingerprints, conduct background checks, verify identity, or retrieve reports, subject to permissible purpose and contractual restrictions.
- **Government, Regulatory, and Law Enforcement Authorities:** Where required or permitted by law (including DOT and other compliance reporting), in response to subpoenas, court orders, or lawful requests, or to protect rights, safety, and integrity of our services.
- **Service Providers and Contractors:** Vendors who support operations such as secure hosting, scheduling systems, communications, analytics, payment processing (if applicable), document management, or customer support—under confidentiality and security obligations.
- **Business Transfers:** If we engage in a merger, acquisition, financing, reorganization, or sale of assets, information may be disclosed as part of the transaction subject to appropriate confidentiality protections and applicable law.

We disclose information on a need-to-know basis and, where applicable, pursuant to written agreements requiring confidentiality, appropriate safeguards, and limited use.

5. DATA STORAGE, SECURITY, AND CHAIN OF CUSTODY

Vantage Verify prioritizes the integrity of every specimen and data point.

- **Chain of Custody:** We adhere to rigorous chain-of-custody protocols designed to ensure results and documentation are legally defensible and resistant to tampering.

- **Data Storage:** Information may be stored in secure electronic systems and/or physical records, depending on the service and regulatory requirements. Access is restricted to authorized personnel with a legitimate business need.
- **Security Measures:** We maintain reasonable and appropriate administrative, technical, and physical safeguards designed to protect information from unauthorized access, disclosure, alteration, and destruction. These safeguards may include access controls, role-based permissions, encryption in transit and/or at rest where appropriate, secure credential practices, audit logging, and staff training.
- **Mobile/On-Site Security:** Our on-site collection and verification processes are designed to maintain privacy and confidentiality in workplace environments, including secure handling and transport of specimens and documentation.
- **Incident Response:** We maintain procedures intended to detect, investigate, and respond to suspected security incidents. Where required by applicable law, we will provide notifications regarding certain data breaches.

No method of transmission or storage is 100% secure; however, we work to maintain safeguards appropriate to the sensitivity of the information.

6. DATA RETENTION

We retain personal information only for as long as reasonably necessary to provide services, comply with legal and regulatory obligations, maintain defensible records (including chain-of-custody), and resolve disputes. Retention periods vary depending on the service, the nature of the information, customer requirements, and applicable law.

- **DOT/Regulatory Records:** Where DOT or other regulations apply, we retain records for the periods required by those rules.
- **Testing and Results Records:** Retained for a period consistent with applicable law, contractual obligations, and operational needs (which may differ for negative vs. non-negative results and for different testing modalities).
- **I-9 Verification Records:** Where we assist with I-9-related services, retention and storage are governed primarily by the employer's legal obligations; we retain our related records as required by contract and applicable law.
- **Fingerprinting/Background Check Records:** Retained consistent with applicable law and vendor/regulatory requirements.
- **Notary Records:** Retained as required by applicable law and our recordkeeping practices.

When information is no longer needed, we take reasonable steps to delete, destroy, or de-identify it in a secure manner, consistent with applicable law and our operational capabilities.

7. INDIVIDUAL RIGHTS AND CHOICES

Depending on your jurisdiction and the context in which we process your information (e.g., employer-mandated services vs. direct-to-consumer services), you may have rights relating to your personal information, including:

- **Access:** Request access to the personal information we maintain about you.
- **Correction:** Request correction of inaccurate or incomplete personal information.
- **Deletion:** Request deletion of personal information, subject to legal, regulatory, and contractual limitations (for example, where we must retain records for DOT compliance, defensible chain-of-custody, or other legal requirements).
- **Restriction/Objection (where applicable):** Request that we limit processing, or object to certain processing, where provided by law.
- **Data Portability (where applicable):** Request a copy of certain information in a portable format, where required by law.

Important note for employer-requested services: Where an employer or other authorized requester engages us to perform testing, I-9 verification, or background checks, we may act as a service provider/processor. In those circumstances, certain requests may need to be directed to your employer or the authorized requester, and our ability to act on requests may be limited by law, contractual requirements, and compliance obligations.

To submit a request, please contact us using the information in Section 11. We may need to verify your identity before fulfilling requests.

8. COOKIES & WEBSITE TRACKING

We use cookies and similar technologies (such as pixels and analytics tools) to operate our website, enhance functionality, understand usage, and improve performance.

- **Types of Cookies:** Cookies may be session cookies (expire when you close your browser) or persistent cookies (remain until deleted or expire).
- **Analytics:** We may use analytics providers to help us understand how visitors use our website (e.g., pages visited, time on site, referring sources). These tools may collect technical identifiers and usage data.
- **Your Choices:** You can control cookies through your browser settings and may be able to opt out of certain analytics through provider tools. Disabling cookies may affect website functionality.

9. HIPAA AND HEALTH/TESTING INFORMATION

Certain information we handle—such as drug and alcohol testing documentation and results—may be considered medical or health-related information. Where applicable and required, we handle such information in a confidential manner and apply safeguards appropriate to its sensitivity.

- **HIPAA:** To the extent Vantage Verify is acting as a "business associate" (as defined by the Health Insurance Portability and Accountability Act of 1996 (HIPAA)) for a covered entity, we will comply with applicable HIPAA requirements and any applicable business associate agreement(s). Not all services or relationships are subject to HIPAA.
- **Employer-Requested Testing:** In many employer-requested testing contexts, results may be governed by DOT rules, state law, contractual requirements, and workplace policies rather than HIPAA. We disclose results only to authorized parties and as permitted/required by law.

10. INTERNATIONAL USERS; GDPR (IF APPLICABLE)

Our services are primarily offered in the United States. If you access our website or services from outside the United States, your information may be processed and stored in the United States (or other jurisdictions where our service providers operate), where privacy laws may differ from those in your location.

If the European Union/European Economic Area/United Kingdom General Data Protection Regulation (GDPR) applies to our processing of your personal data, then (in addition to other disclosures in this Policy):

- **Legal Bases:** We process personal data based on one or more legal bases, such as performance of a contract, compliance with legal obligations, legitimate interests (e.g., security and fraud prevention), and/or consent (where required).
- **Your Rights:** You may have rights to access, correct, delete, restrict processing, object, and data portability, and the right to withdraw consent where processing is based on consent.
- **Supervisory Authority:** You may have the right to lodge a complaint with a data protection authority in your jurisdiction.

11. THIRD-PARTY LINKS

Our website may contain links to third-party sites. Vantage Verify is not responsible for the privacy practices or content of these external websites.

12. UPDATES TO THIS POLICY

We reserve the right to modify this Privacy Policy at any time. Changes will be effective upon posting to our website unless otherwise stated. The "Effective Date" at the top of this Policy indicates when it was last updated. Your continued use of our website or services following any updates constitutes acceptance of the revised policy to the extent permitted by law.

13. CONTACT INFORMATION

For questions regarding this Privacy Policy, to submit a privacy request, or for other privacy inquiries, please contact:

Vantage Verify
Attn: Legal/Compliance Department

Website: http://www.vantageverify.org
Email: compliance@vantageverify.org