

PoliPoll Research AI, LLC

Data Quality & Compliance Framework

Website: polipollresearch.com

Document Class: Technical & Compliance Disclosure

Effective Date: October 2026

At **PoliPoll Research AI, LLC**, we operate a multi-layered, automated data verification and tracking ecosystem designed to support complex, cross-border research pipelines. By leveraging top-tier global sample networks and deploying a strictly anonymized routing architecture, we deliver high-integrity research insights spanning international markets while ensuring absolute data security.

1. Global Reach & Sourcing Diversity

Our data engine eliminates regional and sourcing biases through wide-scale, multi-channel network aggregation built for international research targets.

- **Massive Ecosystem Scale:** We integrate with a highly vetted partner network and an elite proprietary panel base encompassing **over 20 million multi-profiled panelists** cross-vetted across **60+ countries** and fully localized in **over 20 languages**.
- **Organic Regional Recruitment:** Panelists are acquired through diverse, country-specific organic recruitment channels, including localized online communities, niche mobile applications, and targeted multi-channel outreach—completely eliminating the risks of unvetted third-party outsourcing or double-brokered international samples.

2. Privacy-by-Design & Data Isolation

Our infrastructure completely isolates and protects respondent identity, thoroughly mitigating compliance risks for cross-border enterprise studies.

- **Zero PII Collection:** We do not collect, host, or transmit Personally Identifiable Information (PII) within our data workflow. All localized respondent profiles and identity metrics are securely managed natively by downstream, primary suppliers.
- **Anonymized Transaction ID Mapping:** Operating as a secure third-party intermediary, our system intercepts downstream supplier transaction IDs, strips all potential identifying markers, and substitutes them with a dynamic, localized transaction ID framework. Upon survey completion, our platform reconverts our tracking code back to the supplier's original ID to safely pass back final parameters without ever exposing individual data.

3. Point-of-Entry Fraud Defense

Every single survey attempt passes through an automated, real-time security gate before being admitted into a live project environment.

- **Continuous Behavioral Monitoring:** Our backend layers leverage vast continuous system intelligence, monitoring over **5 billion annual survey attempts** globally across international markets.

- **130+ Point Risk Filtering:** Each distinct respondent is evaluated instantly against more than **130 structural fraud signals** at the point of entry. This process actively flags and blocks bots, server farms, malicious scripts, and suspect proxy/geolocation configurations before data collection ever begins.

4. Advanced Quality Controls & Local Optimization

To guarantee high-fidelity data, the data pipeline enforces rigorous automated and human quality oversight layers.

- **16-Layer In-Flight Checks:** Live respondent traffic is evaluated via a **16-point machine learning array** that dynamically tracks speeders, straight-liners, logical inconsistencies, and cross-lingual gibberish text patterns.

- **Dynamic Source Throttling:** Performance metrics are continuously tracked across all integrated sample paths. Underperforming routes are dynamically throttled or suspended in real-time to preserve survey integrity and uphold target metrics.

- **Continuous Human QA Oversight:** Our automated defenses are paired with a dedicated **24/7/365 internal Human Quality Assurance team** that continuously audits open-ended text string submissions and cross-market validation trends.

Technical Appendix: Client Security & Compliance FAQ

Q: How does PoliPoll Research AI, LLC handle respondent Personally Identifiable Information (PII) and GDPR/CCPA compliance?

A: We practice strict data minimization. By design, our internal data workflows do not collect, capture, or host any Personally Identifiable Information (PII). All user-facing profile registries and demographic data stay safely isolated within our downstream primary suppliers' secure environments. Because we never store or process PII on our servers, your enterprise faces zero consumer data liability when launching a study with us.

Q: If a client or respondent requests a complete data deletion, how is it executed?

A: Because we do not host PII internally, we handle data deletions upstream and downstream via our specialized transaction framework: We map and replace our suppliers' original transaction IDs with dynamic, localized internal IDs to instantaneously locate the exact survey session in our data tables using your internal record criteria. We then identify the corresponding downstream supplier transaction ID and immediately issue a formal erasure request to the native sample provider housing that profile.

Q: How do you audit your downstream sample suppliers to ensure data quality?

A: We ensure data integrity by continually monitoring real-time quality metrics rather than relying on static annual checks. Our platform continuously audits routes through an active 16-point machine learning array tracking speeders, straight-liners, and open-ended text gibberish. If a specific sample supplier or regional route falls below our threshold for validation consistency, our system triggers an automated Dynamic Source Throttling protocol, instantly slowing down or completely suspending that path in real-time until manual QA auditing clears it.