

This statement summarizes AltDataEU's data provenance, legal framework, and regulatory compliance posture for hedge funds, asset managers, and institutional due diligence officers.

1. Data Provenance & Legal Source Basis

- **100% Statutory Public Domain Sources:** All data is systematically acquired from official government transparency portals, parliamentary archives, and statutory lobbying registers established by law (e.g., German Lobbyregistergesetz, French Loi Sapin II, EU Interinstitutional Agreement).
- **EU Public Sector Information Directives:** All data collection complies with EU Directive 2019/1024 on open data and the re-use of public sector information.
- **Zero Web Scraping Violations:** Data ingestion utilizes official public REST/OData/SPARQL APIs or publicly published bulk XML/JSON/CSV archives with strict adherence to rate limits and robots.txt.

2. Material Non-Public Information (MNPI) Risk Assessment

Conclusion: ZERO MNPI RISK.

AltDataEU does not harvest confidential, insider, leaked, or non-public financial information. All ingested records are official public disclosures mandated by law and published on statutory public portals. Ingestion timestamps provide verifiable auditability of publication timing.

3. GDPR, PII & Privacy Safeguards

- **B2B & Legal Entity Focus:** The commercial dataset exclusively indexes legal entities, corporations, trade associations, registered expenditures, and aggregate statistics.
- **Zero Consumer PII:** AltDataEU does not collect, hold, or license consumer personal data, credit card receipts, mobile location data, or private citizen PII.
- **Public Official Capacity:** Any indexed names are registered statutory lobbyists or elected public officials acting strictly in their official public capacity as published in statutory registers.

4. Information Security & System Audits

- **Infrastructure:** Hosted on SOC 2 Type II and ISO 27001 certified cloud infrastructure (Supabase / AWS / Vercel).
- **Data Integrity:** All data records are hashed and immutable upon ingestion with cryptographic database constraints ensuring zero post-facto tampering.