DATA & NON-PUBLIC PERSONAL INFORMATION (NPI) POLICY
Last Updated: July 2026

1. Strict Zero-NPI Policy

Division One Compliance, LLC ("D1C") provides corporate-level Bank Secrecy Act (BSA) and Anti-Money Laundering (AML) / Counter-Financing of Terrorism (CFT) compliance documentation, risk assessments, and online training modules. **D1C does not collect, request, receive, store, or process Non-Public Personal Information ("NPI") regarding our clients' individual customers.**

2. Client Responsibilities (Prohibition of NPI Transmission)

D1C's services evaluate high-level organizational structure, risk profiles, and written policies. At no time does D1C require individual consumer financial data, Social Security numbers, account details, or government identification to perform its services. **Clients are strictly prohibited from submitting, uploading, or emailing consumer NPI to D1C.**

3. Inadvertent Disclosure Protocol

If a client inadvertently transmits consumer NPI or unredacted personal financial records to D1C, D1C will:

- Immediately delete and permanently destroy the file upon discovery.
- Notify the client of the inadvertent disclosure so the client may log the event in accordance with their internal security policies.
- Refrain from analyzing or storing any of the transmitted consumer NPI.

4. Protection of Corporate Confidential Information

While D1C does not handle consumer NPI, D1C treats all corporate business records, questionnaire responses, and operational details provided by clients as strictly Confidential Information in accordance with our Terms of Service.