Data Deletion & Retention Policy

AccreDeFi
Self-Serve Compliant Tokenization

Data Deletion and Retention Policy (DDRP V1.0)

1 - Policy Statement & Scope

This policy establishes the rules for handling all non-chain data collected, processed, and stored by the AccreDeFi protocol's off-chain services. The primary goal is to ensure continuous compliance with global data privacy regulations while maintaining the necessary immutable audit trail required for institutional financial operations.

2. Data Categories and Required Retention

Data is classified into three categories based on sensitivity, function, and regulatory retention requirements.

Category A - Financial Instrument and Compliance Ledger (Minimum 7 Years)

This category includes non-PII records necessary for financial accounting, audit, and GRC functions. Retention is mandated for a minimum of seven (7) years to align with global financial record-keeping laws.
• **Data Included:** Transaction records, final TokenBook metadata, GTRN hashes, Liquidation Logs, Fee Distribution Records, and all data committed to the XDC Ordinal Inscription (e.g., Signed Document Hash, Legal Counsel Name, transaction amounts).

Category B - Sensitive PII and Operational Data (Strict Data Minimization)

This category includes personally identifiable information obtained during the verification process. Retention of this data is subject to rapid hard deletion.
• **Data Included:** Full Name, Email, Date of Birth, Raw ID Verification IDs (Plaid-generated), IP Address logs, and the original raw Webhook Payloads.
• **Retention Mandate:** This data will be retained for a maximum of six (6) months postverification or immediately upon resolution of any ongoing compliance audit, whichever is later.

Category C: Immutable On-Chain Anchors (Permanent)

This data is permanently recorded on the blockchain ledger (XDC and TON) and is therefore immutable.
• **Data Included:** The Cryptographic Identity Anchor (GIRN equivalent hash), Smart Contract Addresses, Wallet Migration Links, and final validated status records.
• **Retention Mandate:** This data is Permanent and cannot be deleted or altered.

3. Deletion and Erasure Procedures

The organization enforces distinct protocols for the erasure of data:

1. Hard Deletion of PII (Category B): All data in Category B is subject to permanent erasure (hard deletion) from all active databases and log archives six months after the successful verification or immediately upon a valid regulatory request, provided this deletion does not conflict with Category A mandatory retention. Automated lifecycle management tools are used to enforce this schedule

2. Financial Archival (Category A): After the initial three years of active use, financial records are transitioned to a restricted, encrypted archival storage to maintain the seven-year retention mandate.

3. Right to Erasure: While on-chain data (Category C) cannot be erased, all PII (Category B) is erased upon request, adhering to global privacy laws, provided the erasure does not compromise mandatory financial reporting obligations.

4. Technical and Enforcement Controls

This policy is operationalized through continuous technical controls:

- **Data Encryption:** All data subject to retention is protected by AES-256 encryption at rest and communicated only via TLS 1.2+ connections.
- **Access Control:** Access to sensitive data is governed by multi-factor authentication (MFA) and strict role-based access controls (RBAC).
- **Audit Trail:** All data retention, deletion, and archival events are recorded in a separate, tamperproof audit log to demonstrate compliance with the policy

Contact Details

RegulatedTokens.com	Contact@AccreDefi.Net	AccreDefi