Data Retention and Disposal Policy

Richtlinie zur Datenaufbewahrung und Datenentsorgung · CompanyFin

Operating Entity / Betreiberin: ShiftCore UG (haftungsbeschränkt), Weilstraße 10, 65183 Wiesbaden, Germany
Product / Platform: CompanyFin (B2B SaaS Accounting Platform)
Data Protection Officer & Governance: Tim Prellwitz, Managing Director (Geschäftsführer)
Policy Version: 1.0 | **Effective Date:** September 17, 2026 | **Review Cycle:** Annual

1. Purpose and Regulatory Alignment

This Policy establishes enforceable standards for the retention, archival, and secure disposal of customer, financial, and operational data processed within CompanyFin. It guarantees full compliance with:

- **EU General Data Protection Regulation (GDPR / DSGVO):** Principles of storage limitation (Art. 5(1)(e)), data minimization (Art. 5(1)(c)), and right to erasure (Art. 17).
- **German Commercial Code (HGB § 257) & Fiscal Code (AO § 147):** Statutory 6- and 10-year archival requirements for commercial accounting records and business vouchers.
- **Principles of Proper Computerized Accounting Systems (GoBD):** Immutable electronic storage.
- **Financial API & Partner Security Standards:** Security compliance requirements mandated by **Plaid Inc.** and European Open Banking / PSD2 regulations.
- **NIST SP 800-88 Revision 1:** Guidelines for media sanitization and cryptographic disposal.

2. Scope and Systems

This Policy applies to all digital assets, databases, and third-party integrations operated by ShiftCore UG:

- **Relational Production Databases (PostgreSQL):** User accounts, organizations, transaction ledgers, journals, and audit trails.
- **Cloud Object Storage (Hetzner S3, Region Nürnberg / Germany):** Encrypted receipt images, invoice PDFs, OCR text files, and export archives.
- **Third-Party Banking APIs:** Bank sync credentials, access tokens, and cursors (Plaid, Enable Banking, Stripe Connect).
- **In-Memory Caches & Throttling (Redis):** Ephemeral auth state, rate-limiting counters.
- **Inbound Email Pipelines (Resend):** Receipt processing at `belege.companyfin.de`.

3. Data Classification Matrix

Tier	Description	Examples	Sensitivity
Class 1: Master Data	User identity & organization records.	Company name, full name, email, Argon2/bcrypt password hash.	High
Class 2: Financial Records	Statutory business records & receipts.	Invoices (PDF/PNG), extracted vendor metadata, SKR04 bookings, DATEV files.	Critical (Statutory)
Class 3: Provider Tokens	Credentials enabling bank sync.	Plaid Item IDs, encrypted access tokens, Enable Banking session tokens.	Highly Critical
Class 4: Ephemeral Data	Short-lived session & security states.	HTTP-only session cookies, JWT refresh tokens, OAuth state tokens.	Medium
Class 5: System Logs	Diagnostics & access event logs.	Anonymized IPs, HTTP response codes, Sentry traces (scrubbed).	Low

4. Retention Schedule and Statutory Timelines

Data is stored strictly for the duration required to achieve its operational purpose or to satisfy mandatory statutory retention periods:

Data Category	Retention Period	Statutory Trigger	Legal Ground
Statutory Accounting Records & Invoices	**10 Years**	Close of calendar year of finalized booking	§ 147 Abs. 1 AO; § 257 HGB; GoBD
Commercial Letters & Contracts	**6 Years**	Close of calendar year of dispatch/ receipt	§ 147 Abs. 1 Nr. 2, 3 AO; § 257 HGB
Active Customer Accounts	**Active Contract + 30 Days**	Duration of subscription; 30-day export grace period	Art. 6(1)(b) GDPR
Bank Connection Tokens (Plaid / Bank Sync)	**Immediate Deletion / Invalidation**	Upon user disconnect or account closure	Art. 6(1)(b) GDPR; User Authorization
Temporary Bank Snapshots	**Max 90 Days**	Reconciled into confirmed ledger bookings	Art. 5(1)(c) GDPR (Data Minimization)
Authentication Session Cookies	**15 Min to 30 Days**	15 min access; rolling 30-day refresh or logout	§ 25 Abs. 2 TDDDG
OAuth States & Reset Tokens	**30 to 45 Minutes**	Plaid OAuth state: 45 min; Password reset: 30 min	Ephemeral Token TTL
Security Audit Logs	**12 to 24 Months**	Rolling rotation; intrusion detection & audit	Art. 6(1)(f) GDPR
Error Diagnostics (Sentry)	**90 Days**	Rolling window; request bodies & auth stripped	Art. 6(1)(f) GDPR

5. Account Deletion and Right to Erasure Workflow

5.1 User-Initiated Bank Disconnection

- **Immediate Revocation:** Upstream provider token is revoked via API (e.g. Plaid `/item/remove`).
- **Cryptographic Shredding:** The encrypted access token (`encrypted_access_token`) and sync cursors are permanently purged from the database.
- **No Further Ingestion:** Ingestion terminates immediately. Confirmed accounting bookings remain for tax compliance.

5.2 Account Termination and Cascading Purge

1. **Deactivation & 30-Day Grace Period:** The account enters read-only status for 30 calendar days, allowing customer export of accounting journals (DATEV EXTF format) and receipt archives.
2. **Cascading Database Deletion:** Automated purge routines execute cascading deletions across PostgreSQL, removing user profiles, tenant associations, API keys, and session records.
3. **Object Storage Purge:** Tenant documents and receipt images in Hetzner S3 are irreversibly deleted via API deletion calls.
4. **Customer Statutory Tax Duties:** Under German law, corporate customers (GmbH/UG) bear the legal duty of 10-year archiving. CompanyFin provides full data export capabilities prior to permanent account deletion.

6. Secure Disposal and Sanitization Standards

ShiftCore UG applies data sanitization standards aligned with **NIST SP 800-88 Rev. 1**:

- **Cryptographic Erasure (Crypto-Shredding):** Sensitive financial credentials (Plaid access tokens) are stored encrypted at rest using authenticated symmetric Fernet / AES-128-CBC encryption. Deletion of database records combined with key rotation renders residual data permanently undecipherable.
- **Logical Database Sanitization:** SQL `DELETE` with cascading constraints removes orphaned records. Database instances execute regular `VACUUM FULL` to overwrite physical disk allocations.
- **Object Storage Sanitization:** Hetzner S3 bucket object deletions are permanent and cannot be restored.
- **Physical Infrastructure Disposal:** ShiftCore UG utilizes certified cloud infrastructure. Physical drive decommissioning and destruction are executed by **Hetzner Online GmbH** (ISO/IEC 27001, DIN 66399 mechanical shredding / degaussing) and **Render Services, Inc.** (SOC 2 Type II).
- **Workstation Sanitization:** Administrative workstations enforce full-disk hardware encryption (LUKS / FileVault / BitLocker) and are sanitized using cryptographic wipes prior to reassignment.

7. Legal Holds and Exceptions

Under Article 17(3)(b) GDPR, statutory commercial/tax retention (§ 257 HGB, § 147 AO) supersedes immediate erasure. In case of active tax audits, government subpoenas, or legal disputes, data is segregated under an administrative legal hold until formal conclusion.

8. Periodic Review and Governance

This Policy is reviewed and affirmed **annually** by the Managing Director of ShiftCore UG. Ad-hoc evaluations occur upon significant technical or regulatory changes.
Next Scheduled Review: September 2027.

9. Contact and Policy Administration

ShiftCore UG (haftungsbeschränkt)
Weilstraße 10, 65183 Wiesbaden, Germany
E-Mail: datenschutz@companyfin.de / support@companyfin.de | Phone: +49 1567 9772959

Approved and Enforced by:

Tim Prellwitz
Tim Prellwitz, Managing Director (Geschäftsführer)
ShiftCore UG (haftungsbeschränkt) | Date: September 17, 2026