VLN – Full GDPR Compliance Pack

This document includes public GDPR documentation and internal compliance framework for VLN (Virtual Licensing Network) in accordance with EU Regulation 2016/679.

1. GDPR PUBLIC COMPLIANCE STATEMENT

- VLN processes personal data in compliance with EU Regulation 2016/679 (GDPR).
- Data categories: identification data (name, email), IP address, device metadata, licensing records, audit logs, transaction references.
- Legal basis: contract execution (Art.6(1)(b)), legal obligation (Art.6(1)(c)), legitimate interest (security & fraud prevention), consent (cookies).
- Data subject rights: access, rectification, erasure, restriction, objection, portability.
- Data retention limited to service necessity and legal obligations.
- Data transfers only to verified sub-processors under contractual safeguards.
- No sale of personal data.

2. RECORD OF PROCESSING ACTIVITIES (Art.30 GDPR)

- Controller: VLN – Virtual Licensing Network.
- Purpose: licensing infrastructure, forensic verification, account management, royalty tracking.
- Categories of data subjects: platform users, SaaS enterprise clients, buyers.
- Categories of personal data: identification data, contact data, transaction references, IP logs, audit metadata.
- Recipients: hosting providers (e.g., AWS), payment processors (e.g., Stripe), technical service providers.
- Retention period: active contract duration + legal retention period for financial and audit records.
- Security measures: encryption, hashing (SHA-256), access control, logging, signed audit packs.

3. DATA RETENTION POLICY

- Account data retained for duration of active service.
- Financial records retained according to applicable tax regulations.
- Forensic audit logs retained to preserve system integrity and contractual traceability.
- Inactive accounts subject to deletion or anonymization after defined retention period unless legal obligation applies.

4. DATA BREACH RESPONSE PROCEDURE

- Incident identification and immediate containment.
- Internal investigation and risk assessment.
- Notification to supervisory authority within 72 hours when required.
- Notification to affected data subjects when high risk is identified.
- Incident documentation and corrective action implementation.

5. SUB-PROCESSOR LIST

- Cloud Infrastructure Provider (e.g., AWS).
- Payment Processor (e.g., Stripe).
- Content Delivery Network (CDN provider if applicable).
- Email Delivery Provider (if applicable).
- All sub-processors subject to contractual data protection obligations.

6. TECHNICAL & ORGANIZATIONAL MEASURES (TOMs)

- Encryption in transit (HTTPS/TLS).
- Encryption at rest for sensitive data.
- Cryptographic hashing for asset verification (SHA-256).
- Digital signature for audit packs.
- Role-based access control (RBAC).
- Append-only ledger architecture for traceability.
- Logging & monitoring for anomaly detection.
- Regular backup and disaster recovery procedures.