IPrio

Security & Compliance

Built for Safety. Designed for Trust.

IPrio is engineered to protect your creative work with enterprise-grade security and modern compliance standards. From file upload to certificate generation, every step is built on encryption, strict privacy controls, and auditable technology.

Your files stay private. Your data stays secure. Your proof stays verifiable.

Our Security Standards

End-to-End Encryption

All data is encrypted:

- **In transit:** HTTPS + TLS 1.2+
- **At rest:** Secure encrypted storage
- **Internally:** Strict access isolation to prevent unauthorized access

Your files are never shared, indexed, or exposed.

Cryptographic Hashing

Every upload receives a **unique cryptographic fingerprint (hash)**.
This ensures:

- Tamper-proof verification
- Content authenticity
- Zero exposure of the file itself

Only the hash - not the file - ever leaves the secure environment.

Trusted Timestamps (TSP)

IPrio partners with **EU-compliant Trusted Service Providers (TSPs)** to issue official timestamps recognized under eIDAS.

This adds a legally credible time-mark to your work.

Blockchain Anchoring

Every file hash is also written to a public blockchain, providing:

- Immutable proof
- Decentralized verification
- Long-term auditability

No personal data or file content is ever placed on the blockchain.

Compliance & Data Protection

GDPR Compliant

IPrio follows GDPR principles for:

- Data minimization
- Purpose limitation
- User rights
- Transparency

Users can request:

- Data access
- Data deletion
- Export of personal information
- Account removal

Privacy by Design

IPrio's architecture follows:

- Minimum necessary data processing
- Content non-access (we never open your files)
- Separation of storage and hashing layers
- Secure identity & session handling

Independent Verifiability

Your timestamps and blockchain records are verifiable by:

- Third-party TSP tools
- Public blockchain explorers
- Internal IPrio verification tools

This ensures transparency without leaking private content.

Secure Infrastructure

We host and operate on trusted cloud providers with:

- Redundant storage
- Distributed backups
- DDoS protection
- Access control policies
- Continuous monitoring

Platform Integrity & Abuse Prevention

Continuous Monitoring

We monitor the system for:

- Anomalies
- Malicious uploads
- Unauthorized access attempts

Prohibited Use

We prohibit:

- Malware
- Illegal content
- Anti-moral behavior
- Infringing materials

- Automated abuse

Violations may lead to account suspension under our Terms.

Incident Response

If a security incident occurs, we will:

1. Identify and isolate the issue
2. Resolve and secure affected systems
3. Notify impacted users (if applicable)
4. Provide remediation steps

Our goal: transparency, speed, and user protection.

Have Questions About Security?

We're here to help.
Contact our Security & Compliance team at:
support@iprio.io