IPFN: Governance, Trust and Data Protection

Who checks the claim? Who corrects a mistake?

Problem: A permanent record can preserve a false claim, too.

Our approach: Show the evidence. Name the operator. Provide a challenge process.

IPFN gives a registered work a web address. Someone opening it can see who claimed the work and which file was registered, then inspect the certificate and ledger evidence. For institutional use, we also need clear answers to ordinary questions: who accepts a registration, who can challenge a false claim, who corrects a mistake, who protects personal data, and who remains responsible if the operator fails?

This paper proposes that operating framework. Blinding Visuals Press operates the present reference service. Independent agency governance, additional registrars, and public-interest oversight are proposed next steps. They are not represented here as already established.

1. Keep three questions separate

Who made the claim? An account, email address, identity check, and institutional attestation provide different levels of assurance. The public record should state which check occurred and when. An authenticated account is not automatically a verified legal identity, and a verified legal identity does not establish authorship.

Which file does the claim concern? SHA-256 provides an exact-file fingerprint. Matching bytes can be checked against that value. A resized or recompressed image can be visually similar while producing a different hash. Similarity detection can help find candidates for review; it does not decide who owns the underlying work.

What has been preserved? A pinned certificate and a completed ledger anchor are different evidence states. The public interface must show each state honestly. A reader should be able to inspect the certificate record, obtain the canonical ledger, recalculate its hash, and compare that commitment with the public transaction.

2. Register claims without making registration a gate

Copyright protection generally arises without registration. Voluntary records can support evidence and rights discovery while respecting that principle. The proposed IPFN framework therefore makes participation optional, preserves the creator's rights, and treats an absent record as an absent record - never as evidence that a work is unprotected. Existing national copyright offices, collecting societies, publishers, and specialist registries retain their roles. [1]

IPFN should publish its identifier rules, essential schema, verification procedure, registrar requirements, revision history, and exit arrangements. A creator should be able to export the record and supporting evidence without buying a new service. Institutions should be able to connect to the same public specification through more than one operator.

The agency's proposed job is to maintain those common rules and oversee participation. The operator's job is to run the technology. A dispute review body's job is to examine challenged records. Keeping those roles explicit makes accountability possible even while the reference implementation begins under one operator.

3. Build a dispute process around the hard case

Consider a stolen photograph registered before its creator notices. The first timestamp proves that a record existed; it does not make the claimant the author. A serious registry must handle that case without turning its own speed into a reward for fraud.

The proposed process is straightforward. Accept a challenge through a public channel. Identify the exact record and the challenger's asserted interest. Preserve relevant evidence. Notify the claimant where lawful and appropriate. Mark the public record as disputed once the published threshold is met. Give each side a chance to respond. Have a reviewer who is not deciding their own commercial dispute issue a reasoned outcome, with an appeal route.

Possible outcomes include a correction, an added competing claim, a restricted public projection, withdrawal of an unsupported claim, or referral to the competent legal process. The record must distinguish an operator action from a court decision. A correction should explain what changed and why, without unnecessarily exposing private evidence. Abuse reports and identity documents belong in controlled case files, not permanent public certificates.

These are pilot acceptance requirements. This paper does not claim that every proposed step is already available in the beta service.

4. Use blockchain as a public witness

We use blockchain for a practical evidence function: commit the fingerprint of a ledger so that another party can inspect the same public commitment. In that sense, it performs a notary-like role. It provides a reference outside the operator's editable database.

The legal distinction matters. A blockchain does not interview the claimant, authenticate the underlying facts, or turn a private record into a notarial act. In AZ Factory v Valeria Moda, the Marseille court considered blockchain timestamp reports together with corroborating evidence in a copyright dispute. The case supports carefully documented digital evidence; it does not establish blanket equivalence to a legal notary or endorse IPFN. The correct citation is Tribunal judiciaire de Marseille, First Civil Chamber, 20 March 2025, RG 23/00046. [2]

EU law separately addresses ordinary and qualified electronic timestamps and ledgers. The legal presumptions associated with qualified services depend on the applicable requirements and qualified provider status. IPFN does not claim that status in this paper. An institution can evaluate whether an additional qualified trust-service layer is useful for its own evidentiary requirements. [3]

5. Decide what should be public before publishing it

The institutional model should minimize public personal data by design. A creator should see the exact public projection before agreeing to publish a record. The proposed data separation is:

Layer	Purpose	Proposed treatment
Public discovery record	Identifier, work description, claimant display name, rights/contact route, evidence status	Publish only necessary fields, with clear notices and correction mechanisms.
Private claimant file	Account details, identity evidence, contact information, declarations	Controlled access, defined retention, and an appropriate lawful basis.

Layer	Purpose	Proposed treatment
Private dispute file	Challenges, correspondence, supporting documents, reviewer decisions	Restricted case access, recorded reasons, and retention tied to the dispute and legal duties.
Public certificate/IPFS record	Portable evidence associated with the registration	Use the minimum justified content; explain replication and limits on withdrawal before publication.
Public chain commitment	Evidence of integrity and chronological commitment	Avoid directly identifying personal data; evaluate linkability and necessity rather than assuming a hash is anonymous.

This is a target design, not a statement that all historical records can be retracted. A public IPFS copy may persist with third parties after an operator stops pinning it. A chain transaction cannot normally be recalled. Those properties must inform the design before sensitive data is published.

6. Make data protection operational

The controller must identify its purposes and lawful bases, provide readable notices, assign processor responsibilities, maintain the relevant processing record, apply proportionate security, and operate rights-request and incident procedures. The exact division of controller, joint-controller, and processor roles follows what each participant actually determines; it cannot be settled by a label in a marketing document. [4]

For the institutional pilot we propose a documented data-flow review before onboarding, a data protection impact assessment wherever required, and independent review of unresolved risks. The review should cover public replication, identity checks, disputed claims, personal data within photographs, deletion and correction, key management, recovery, and international transfers. The EDPB's final blockchain guidance, adopted7 July 2026, is the current reference; technical immutability is not an exemption from data protection obligations. [5]

The EU hosting question needs the same discipline. Database location alone does not establish EU-only processing. The inventory must identify every IPFN-related database, source store, preview store, worker, gateway, analytics service, backup, support-access path, and subprocessor. For each one, record the fields, processing purpose, region, retention, access arrangements, and any transfer mechanism. An institutional deployment can then be scoped around an agreed European operating model. This paper makes no blanket claim that the current beta is already EU-only or independently certified as GDPR compliant.

7. Commission the institution-facing service

Before an institutional pilot expands, the parties should inspect a real registration, a changed file, an unavailable gateway, a delayed anchor, a challenged claim, a correction, an export, a rights request, and an operator recovery exercise. Each should end in a visible, understandable outcome.

Publish the resulting service measures: successful record resolutions, certificate availability, anchor delay, disputed-record handling, correction time, false-positive rates for any similarity system, and export completeness. Name the operator responsible for a failure and the party that verifies recovery. Publish a succession plan so that identifiers and evidence do not depend on one founder, one domain renewal, or one service provider indefinitely.

The goal is simple: a creator registers a work; a reader opens its identifier to inspect the claim and file evidence; and an institution knows who must fix a mistake. That is the service we propose testing.

References

[1] WIPO, Copyright Registration Systems. https://www.wipo.int/en/web/copyright/activities/copyright-registration/index

[2] TJ Marseille,1st Civil Chamber, 20 March 2025, AZ Factory v Valeria Moda, RG 23/00046; judgment reproduced by Legalis. https://www.legalis.net/jurisprudences/tribunal-judiciaire-de-marseille-1ere-ch-civile-jugement-du-20-mars-2025/ . EUIPO case summary: https://www.euipo.europa.eu/de/law/recent-case-law/he-court-of-marseille-recognised-blockchain-timestamping-as-legitimate-evidence-of-copyright-ownership

[3] Regulation (EU) 910/2014,Article 41: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX%3A32014R0910 ; Regulation (EU) 2024/1183,Articles 45k-45l: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A32024R1183

[4] GDPR,Regulation (EU) 2016/679,Articles 5, 6, 12-22, 25, 28, 30, 32-36, 44-49. https://eur-lex.europa.eu/legal-content/ENG/ALL/?uri=celex%3A32016R0679

[5] EDPB, Guidelines 02/2025 on processing of personal data through blockchain technologies,final v2,7 July 2026. https://www.edpb.europa.eu/documents/guideline/guidelines-022025-on-processing-of-personal-data-through-blockchain_en ; DPIA guidance: https://www.edpb.europa.eu/topics/accountability-and-compliance-tools/data-protection-impact-assessment_en