AI CURATOR
CURATING THE FUTURE OF AI

Data Compliance Checklist

Use this checklist to verify that all datasets meet essential privacy, security, and regulatory requirements before being used in AI workflows.

1. Privacy Requirements

- All Personally Identifiable Information (PII) identified and documented.
- PII masked, encrypted, or removed where required.
- Consent collected for any user data included in the dataset.
- Data collection practices match published privacy policies.

2. Security Requirements

- Dataset stored in secure, access-controlled environment.
- Encryption applied at rest and in transit.
- Access limited to authorized team members only.
- Audit logs enabled for all data interactions.

3. Legal & Regulatory Compliance

- Dataset reviewed for GDPR relevance.
- Dataset reviewed for CCPA/CPRA requirements.
- Dataset compliant with HIPAA (if applicable).
- Industry-specific standards reviewed and followed (FINRA, SOC2, PCI, etc.).

4. Data Integrity & Handling

- Data retention policy reviewed and followed.

- Deletion requests are processed and documented.

- Data lineage tracked (source → transformation → output).

- Backup and recovery processes verified.

5. Third-Party & Vendor Checks

- All third-party data sources are verified as compliant.

- Vendor contracts reviewed for data protection clauses.

- Data transfer agreements (DPAs) in place where needed.

6. Risk Assessment

- Potential risks identified (privacy leaks, bias, misuse).

- Risk mitigation steps documented.

- Incident response plan in place for data breaches.

- Compliance checklist reviewed and approved by stakeholder.