# Data Governance Compliance Checklist

Project Name: [Insert Project Name]

Date: [Insert Date]

Version: [Insert Version Number]

**1. Introduction**

This Data Governance Compliance Checklist is designed to ensure that all data used in the [Insert Project Name] complies with established governance policies, including data quality, privacy, and security standards. This checklist serves as a comprehensive guide to verify that data handling practices align with organizational and regulatory requirements throughout the ML lifecycle.

**2. Purpose**

The purpose of this checklist is to:

* Ensure that data used in the [Insert Project Name] meets the required standards for quality, privacy, and security.
* Facilitate consistent adherence to data governance policies across all phases of the ML lifecycle.
* Identify and address any compliance gaps or risks associated with data usage.

**3. Checklist Overview**

The checklist is divided into the following sections:

* Data Quality Compliance
* Data Privacy Compliance
* Data Security Compliance
* Documentation and Audit Compliance

Each section contains specific criteria to verify compliance with relevant policies and standards.

**4. Data Quality Compliance**

This section ensures that data used in the [Insert Project Name] meets quality standards, including accuracy, completeness, consistency, and timeliness.

|  |  |  |
| --- | --- | --- |
| Criteria | Status | Comments |
| 4.1 Data Accuracy |  |  |
| a. Data accurately represents the real-world entities or phenomena it describes. | Compliant  Non-Compliant | [Add Comments] |
| b. Data validation checks are performed to identify and correct inaccuracies. | Compliant  Non-Compliant | [Add Comments] |
| 4.2 Data Completeness |  |  |
| a. All necessary data elements are present and accounted for. | Compliant  Non-Compliant | [Add Comments] |
| b. Missing data is identified, and appropriate handling techniques are applied (e.g., imputation, exclusion). | Compliant  Non-Compliant | [Add Comments] |
| 4.3 Data Consistency |  |  |
| a. Data is consistent across different sources and systems. | Compliant  Non-Compliant | [Add Comments] |
| b. Data integration processes ensure consistency in data format and structure. | Compliant  Non-Compliant | [Add Comments] |
| 4.4 Data Timeliness |  |  |
| a. Data is up-to-date and reflects the most current information available. | Compliant  Non-Compliant | [Add Comments] |
| b. Data refresh schedules are followed to maintain timeliness. | Compliant  Non-Compliant | [Add Comments] |

**5. Data Privacy Compliance**

This section verifies that data privacy standards are met, ensuring compliance with relevant regulations such as GDPR, CCPA, and other data protection laws.

|  |  |  |
| --- | --- | --- |
| Criteria | Status | Comments |
| 5.1 Data Anonymization and Pseudonymization |  |  |
| a. Personally identifiable information (PII) is anonymized or pseudonymized as required. | Compliant  Non-Compliant | [Add Comments] |
| b. Anonymization techniques effectively prevent re-identification of individuals. | Compliant  Non-Compliant | [Add Comments] |
| 5.2 Data Consent and Usage Rights |  |  |
| a. Consent has been obtained for the use of personal data, where applicable. | Compliant  Non-Compliant | [Add Comments] |
| b. Data usage is consistent with the purposes for which consent was obtained. | Compliant  Non-Compliant | [Add Comments] |
| 5.3 Data Subject Rights |  |  |
| a. Data subjects have been informed of their rights (e.g., access, correction, deletion). | Compliant  Non-Compliant | [Add Comments] |
| b. Processes are in place to respond to data subject requests promptly. | Compliant  Non-Compliant | [Add Comments] |
| 5.4 Compliance with Data Protection Regulations |  |  |
| a. Data handling practices comply with relevant data protection regulations (e.g., GDPR, CCPA). | Compliant  Non-Compliant | [Add Comments] |
| b. Regular audits are conducted to ensure ongoing compliance with privacy laws. | Compliant  Non-Compliant | [Add Comments] |

**6. Data Security Compliance**

This section ensures that data is protected from unauthorized access, breaches, and other security threats.

|  |  |  |
| --- | --- | --- |
| Criteria | Status | Comments |
| 6.1 Data Encryption |  |  |
| a. Data is encrypted at rest and in transit using industry-standard encryption methods. | Compliant  Non-Compliant | [Add Comments] |
| b. Encryption keys are securely managed and rotated regularly. | Compliant  Non-Compliant | [Add Comments] |
| 6.2 Access Controls |  |  |
| a. Access to data is restricted based on roles and responsibilities (e.g., Role-Based Access Control). | Compliant  Non-Compliant | [Add Comments] |
| b. Multi-factor authentication (MFA) is required for accessing sensitive data. | Compliant  Non-Compliant | [Add Comments] |
| 6.3 Security Monitoring and Incident Response |  |  |
| a. Security monitoring tools are in place to detect and respond to potential threats. | Compliant  Non-Compliant | [Add Comments] |
| b. Incident response procedures are documented and regularly tested. | Compliant  Non-Compliant | [Add Comments] |
| 6.4 Data Backup and Recovery |  |  |
| a. Regular backups of data are performed and securely stored. | Compliant  Non-Compliant | [Add Comments] |
| b. Data recovery procedures are in place and regularly tested to ensure data integrity. | Compliant  Non-Compliant | [Add Comments] |

**7. Documentation and Audit Compliance**

This section ensures that all necessary documentation is maintained, and regular audits are conducted to verify compliance with data governance policies.

|  |  |  |
| --- | --- | --- |
| Criteria | Status | Comments |
| 7.1 Data Lineage Documentation |  |  |
| a. Data lineage is documented, tracking the origin, flow, and transformations of data. | Compliant Non-Compliant | [Add Comments] |
| b. Data lineage documentation is regularly updated to reflect changes in data flows. | Compliant Non-Compliant | [Add Comments] |
| 7.2 Data Governance Policies and Procedures |  |  |
| a. Data governance policies and procedures are documented and accessible to all relevant stakeholders. | Compliant Non-Compliant | [Add Comments] |
| b. Policies and procedures are regularly reviewed and updated to reflect best practices and regulatory changes. | Compliant Non-Compliant | [Add Comments] |
| 7.3 Audit Trails and Logs |  |  |
| a. Audit trails are maintained for all data access and modifications, ensuring traceability. | Compliant Non-Compliant | [Add Comments] |
| b. Logs are regularly reviewed to identify and address any unauthorized access or anomalies. | Compliant Non-Compliant | [Add Comments] |
| 7.4 Regular Compliance Audits |  |  |
| a. Regular compliance audits are conducted to verify adherence to data governance policies. | Compliant Non-Compliant | [Add Comments] |
| b. Findings from audits are documented, and corrective actions are implemented as needed. | Compliant Non-Compliant | [Add Comments] |

**8. Review and Sign-Off**

This section confirms that the Data Governance Compliance Checklist has been reviewed and approved by the relevant stakeholders.

|  |  |  |  |
| --- | --- | --- | --- |
| Reviewer Name | Role | Date | Signature |
| [Insert Reviewer Name] | [Insert Role] | [Insert Date] | [Insert Signature] |
| [Insert Reviewer Name] | [Insert Role] | [Insert Date] | [Insert Signature] |
| [Insert Reviewer Name] | [Insert Role] | [Insert Date] | [Insert Signature] |

**9. Document Control**

* Document Owner: [Insert Name, Role]
* Approval Date: [Insert Date]
* Next Review Date: [Insert Date]
* Version History:
  + Version [Insert Version Number] - Initial Document - [Insert Date] - Approved by [Insert Name]