



IntelliSync AI Data Privacy Checklist

Essential Checklist for Ensuring Data Privacy Compliance in AI Projects

Prepared by IntelliSync Solutions

Introduction

Data privacy compliance is critical for the successful implementation of AI projects. This checklist ensures that organizations follow best practices, align with relevant regulations, and safeguard sensitive information throughout the AI lifecycle.

1. Data Collection & Consent

- Obtain explicit user consent for data collection.
- Provide clear privacy notices and opt-out mechanisms.
- Collect only data necessary for the defined purpose.

2. Data Governance & Policies

- Define data ownership and accountability.
- Maintain updated privacy and data use policies.
- Conduct periodic data governance audits.

3. Security Measures

- Encrypt sensitive data at rest and in transit.
- Apply role-based access controls.
- Regularly update and patch systems handling data.

4. Data Minimization & Retention

- Avoid excessive data collection beyond project needs.
- Define and enforce data retention schedules.
- Securely delete or anonymize data after use.

5. Regulatory Compliance

- Comply with GDPR, PIPEDA, CCPA, or other regional regulations.
- Maintain records of processing activities.
- Conduct Data Protection Impact Assessments (DPIAs) for high-risk AI use cases.

6. Training & Awareness

- Provide regular privacy and security training.
- Raise awareness of phishing and social engineering risks.
- Designate a Data Protection Officer (DPO) if required.

7. Monitoring & Continuous Improvement

- Establish incident response protocols for data breaches.
- Continuously monitor AI systems for compliance.
- Regularly update practices based on new regulations and risks.

Prepared by IntelliSync Solutions

intellisync.io