

COMPLIANCE

AI Security & Compliance Checklist

Ensure your AI implementation meets data privacy, security, and regulatory requirements

23 checklist items

How to use this checklist:

Work through each item in order. Check off completed tasks as you go. Items marked [!] are critical - do not skip them. Share this checklist with your team and assign owners to each section for accountability.

About GetServices.ai

GetServices.ai is the AI services marketplace connecting businesses with vetted AI experts, tools, and implementation support. Our resources are free to use and share. Visit getservices.ai to explore AI services.

AI Security & Compliance Checklist

Data Governance

- ☐  Classify all data that will flow into the AI system (PII, PHI, financial, public).
- ☐  Document a data flow diagram showing where data enters, is processed, and is stored.
- ☐  Confirm data minimization: only collect and process data the AI actually needs.
Note: GDPR Article 5(1)(c) requires data minimization by design.
- ☐  Establish a data retention schedule and automated deletion process.
- ☐  Document the legal basis for processing personal data (consent, legitimate interest, contract).

Access Control

- ☐  Implement role-based access control (RBAC) - limit who can access AI outputs and training
- ☐  Enable multi-factor authentication (MFA) for all admin accounts.
- ☐  Audit and log all access to AI systems - retain logs for minimum 90 days.
- ☐ Implement least-privilege access: users only see data relevant to their role.

Model Security

- ☐  Test for prompt injection attacks - attempt to override system instructions via user input.
Note: Prompt injection is the most common AI-specific attack vector.
- ☐  Implement output filtering to prevent the AI from returning sensitive data (SSNs, passwords, ~~keys~~).
- ☐ Test for model inversion attacks if using a custom-trained model.
- ☐ Establish a process for model updates - test security after every model version change.

Regulatory Compliance

- ☐ **!** If processing EU data: complete a Data Protection Impact Assessment (DPIA).
- ☐ **!** If handling PHI: confirm HIPAA Business Associate Agreement (BAA) is signed with AI vendor.
- ☐ **!** If in financial services: confirm AI decisions comply with fair lending / anti-discrimination laws.
- ☐ **!** Document AI use in your privacy policy and update your cookie consent if applicable.

Incident Response

- ☐ **!** Define an AI-specific incident response plan covering data breach, model failure, and bias
- ☐ Assign an AI incident response owner and document escalation contacts.
- ☐ Test the incident response plan with a tabletop exercise before go-live.
- ☐ **!** Confirm breach notification timelines: GDPR requires 72-hour notification to supervisory
- ☐ **!** Establish a process to disable or roll back the AI system in under 30 minutes if needed.
- ☐ Document third-party AI vendor incident notification obligations in your contract.