AI Compliance Checklist

EMPYREAN RESEARCH INSTITUTE

As organizations accelerate AI adoption, ensuring compliance with legal, regulatory, and ethical standards is paramount. This checklist is designed to help AI teams and legal departments navigate the complexities of data privacy, security, bias, and accountability throughout the AI lifecycle.

Following this structured guide will enable you to build AI solutions that not only comply with regulations but also align with your organization's values and priorities.

1. Data Privacy:

WHAT TO DO: *Ensure data collection, processing, and storage practices comply with applicable privacy laws, such as GDPR (General Data Protection Regulation) and CCPA/CPRA (California Consumer Privacy Act/California Privacy Rights Act).*

ACTION STEPS:

- *Conduct a Data Protection Impact Assessment (DPIA) to identify privacy risks early.*
- *Ensure all personal data is anonymized or pseudonymized where possible.*
- *Establish data retention policies to store data only as long as necessary and legally permitted.*
- *Develop a data breach response plan to handle any potential data leaks efficiently.*

2. Data Minimization:

WHAT TO DO: *Use only the minimum amount of data necessary for the AI model's function. Avoid collecting excessive or irrelevant data that could expose the organization to unnecessary compliance risks.*

ACTION STEPS:

- *Perform a data inventory audit to determine essential data needs.*
- *Regularly review and adjust the scope of data collection based on the principle of minimization.*

3. Consent and Transparency:

WHAT TO DO: *Obtain explicit user consent for data use and ensure transparency around how AI systems handle their data.*

ACTION STEPS:

- *Provide clear, concise privacy notices and consent forms.*
- *Implement granular consent options that allow users to control specific data uses.*
- *Maintain records of user consent for compliance audits.*

4. Security Measures:

WHAT TO DO: *Ensure AI systems are secure, using encryption, access controls, and robust security protocols to safeguard sensitive data.*

ACTION STEPS:

- *Apply end-to-end encryption to protect data in transit and at rest.*
- *Conduct regular penetration testing to assess vulnerabilities.*
- *Assign a Data Protection Officer (DPO) to oversee AI security practices.*

5. Bias Mitigation:

WHAT TO DO: *Design AI models to avoid discriminatory outcomes, especially in sensitive areas like hiring, finance, or healthcare.*

ACTION STEPS:

- *Implement bias detection algorithms and conduct regular bias audits.*
- *Train AI on diverse and representative data sets.*
- *Review AI decision-making for fairness and adjust training data if bias is detected.*

6. Accountability:

WHAT TO DO: *Assign clear responsibility for monitoring and maintaining compliance throughout the AI lifecycle.*

ACTION STEPS:

- *Create an AI Ethics Committee or assign AI oversight responsibilities to a cross-functional team.*
- *Maintain comprehensive documentation for each AI project, detailing design, data usage, and compliance strategies.*
- *Implement a user appeal process for AI-driven decisions that affect individuals.*

EMPYREAN

7. Post-Launch Audits:

WHAT TO DO: Conduct regular post-launch audits to ensure the AI system remains compliant as it evolves and new regulations arise.

ACTION STEPS:

- *Establish a post-launch audit schedule (e.g., quarterly).*
- *Monitor and review key AI performance metrics to ensure compliance with privacy, security, and bias standards.*
- *Use automated compliance tools to monitor for risks and anomalies in real time.*

8. Review Ethical AI Principles:

WHAT TO DO: Ensure AI models align with your organization's ethical standards around fairness, transparency, and accountability.

ACTION STEPS:

- *Develop a set of ethical AI principles based on organizational values (e.g., transparency, fairness, non-discrimination).*
- *Ensure explainability in AI models—users should be able to understand how decisions are made.*
- *Conduct ethical impact assessments to determine how AI decisions affect different user groups.*

9. Review Vendor and Third-Party AI Systems:

WHAT TO DO: Perform due diligence on any external vendors or third-party AI systems to ensure they meet your organization's security, compliance, and ethical standards.

ACTION STEPS:

- *Perform a vendor compliance audit to ensure third-party AI systems comply with relevant data privacy laws (GDPR, CCPA/CPRA).*
- *Ensure that data processing agreements (DPAs) are in place to govern data use and responsibilities between your organization and the vendor.*
- *Review third-party AI models for biases and fairness before integrating them into your systems.*

A Living Document

This checklist is designed to be a living document, evolving alongside your organization's AI projects and the ever-changing regulatory landscape. By following these steps, your team will not only ensure compliance but also promote ethical, responsible AI development. Involve your legal team early and maintain transparency throughout the process to build AI systems that are both innovative and trustworthy.

ABOUT

The Empyrean Research Institute empowers organizations to transform their workforce through evidence-based, innovative insights and real, actionable strategies for a connected, future-ready culture.