AI Ethics & Data Privacy Checklist

A Practical Guide for Responsible AI Adoption

By Justin P. Barrett | justinbarrett.com | Alive LLC

Why This Matters

AI tools process your company's data, your customers' data, and your employees' data. Getting this wrong can mean legal liability, customer trust violations, and reputational damage. This checklist ensures you adopt AI responsibly.

Before Adopting Any AI Tool

- & Read the tool's privacy policy — specifically: is your data used for model training?
- & Check for SOC 2 Type II certification or equivalent security standard
- & Verify data residency — where is your data stored geographically?
- & Confirm data encryption at rest and in transit
- & Check if you can delete your data and get confirmation of deletion
- & Review the tool's data retention policy — how long do they keep your data?
- & Verify the tool is compliant with regulations that apply to you (GDPR, CCPA, HIPAA, etc.)

Data Handling Guidelines

- & Never input customer PII (personally identifiable information) into free-tier AI tools
- & Use enterprise/business tiers that offer data privacy guarantees
- & Anonymize or pseudonymize sensitive data before AI processing
- & Never input trade secrets, source code, or confidential financial data into public AI tools
- & Maintain a log of what data is shared with which AI tools
- & Use API access instead of web interfaces when handling sensitive data (more control)

AI Output Quality & Bias

- & Never publish AI-generated content without human review
- & Check AI outputs for factual accuracy — AI confidently states incorrect information
- & Review AI-generated content for bias (gender, racial, cultural, or political)
- & Don't use AI for final hiring decisions, credit decisions, or legal judgments without human oversight
- & Test AI tools with diverse inputs to check for inconsistent or biased behavior
- & Disclose AI involvement when legally required or ethically appropriate

Employee AI Policy Essentials

- & Publish a clear AI usage policy and distribute to all employees
- & Define which AI tools are approved for company use
- & Specify what types of data can and cannot be shared with AI tools
- & Require human review before any AI output reaches customers
- & Provide AI training so employees know how to use tools effectively and safely
- & Create a process for employees to report AI-related concerns

Customer-Facing AI

- & Disclose when customers are interacting with AI (not a human)
- & Provide easy escalation to a human agent
- & Don't collect more customer data through AI than necessary
- & Ensure AI responses are accurate — wrong information erodes trust fast
- & Monitor AI customer interactions regularly for quality
- & Have a plan for when the AI makes a mistake (it will)

Ongoing Governance

- & Quarterly review of all AI tools in use and their data practices
- & Annual update of AI usage policy
- & Track regulatory developments in AI (EU AI Act, state laws, industry regulations)
- & Maintain an AI tools register: tool name, purpose, data access, owner, renewal date
- & Budget for AI governance as a line item, not an afterthought

About the Author

Justin P. Barrett is an entrepreneur, artist, and author. As CEO of Eyesafe, he built the global standard for display health technology. As founder of Alive LLC, he helps lean teams implement AI systems that actually work — agent architectures, knowledge bases, and automation workflows.

justinbarrett.com | justin@justinbarrett.com