



# AI LEGAL CONSIDERATIONS

## KEY CHECKLIST

*For Business Owners, Corporate Executives & In-House Counsel*

AI is transforming business at unprecedented speed—bringing both opportunity and legal complexity. This checklist identifies critical considerations every organization should address. While internal teams play a vital role, the specialized nature of AI law often requires **partnership with experienced external counsel** to navigate effectively.

### 1. GOVERNANCE & COMPLIANCE

#### ☐ Establish AI Oversight Structure

Determine who has authority and accountability for AI initiatives—whether an AI Ethics Board, executive sponsor, or governance committee with clear decision-making authority.

#### ☐ Identify Applicable Regulations

Map AI applications to relevant federal oversight (FTC, SEC, FDA), state requirements, and industry-specific rules (HIPAA, fair lending, EEOC guidance on hiring tools).

#### ☐ Implement Compliance Documentation

Maintain records demonstrating due diligence: AI system capabilities and limitations, audit trails of decisions, and evidence of compliance efforts.

#### ☐ Monitor Regulatory Developments

AI regulations are evolving rapidly at federal, state, and international levels. Establish processes to track changes affecting your industry and jurisdictions.

### 2. INTELLECTUAL PROPERTY & DATA

#### ☐ Clarify AI-Generated Content Ownership

The U.S. Copyright Office requires human authorship for protection. Establish clear policies and address ownership explicitly in all employment, vendor, and client agreements.

#### ☐ Protect Proprietary AI Innovations

Evaluate patent, trade secret, and copyright strategies. AI patents must demonstrate concrete technical applications; implement trade secret protections for algorithms and training data.

☐ **Ensure Data Privacy Compliance**

AI processing personal data must comply with CCPA, GDPR (if serving EU residents), and other privacy laws granting consumers rights over their data.

☐ **Implement Data Security Measures**

AI systems are high-value cyberattack targets. Deploy multi-layered security including encryption, access controls, and AI-specific incident response plans.

### 3. RISK MANAGEMENT & LIABILITY

☐ **Conduct AI Risk Assessment**

Before deployment, identify risks across data privacy, discriminatory outcomes, system errors, reputational harm, and regulatory non-compliance with documented mitigation strategies.

☐ **Establish Accountability Frameworks**

Define who is responsible when AI systems affect customers, employees, or third parties. Clear accountability prevents gaps that create liability exposure.

☐ **Review Insurance Coverage**

Traditional policies may not cover AI risks. Evaluate specialized AI/technology insurance and document coverage requirements in vendor and client agreements.

☐ **Prepare for Litigation**

AI-related litigation is increasing. Maintain comprehensive documentation of development, testing, training data provenance, and compliance efforts.

### 4. CONTRACTS & EMPLOYMENT

☐ **Review AI Vendor Agreements**

Negotiate data ownership, usage rights, liability allocation, and compliance obligations. Standard vendor terms rarely favor the customer—careful review is essential.

☐ **Address AI in Client Contracts**

If deliverables include AI-generated content, explicitly address ownership, quality standards, and limitations. Ambiguity creates expensive disputes.

☐ **Audit AI Hiring Tools for Bias**

AI recruiting tools can perpetuate historical biases, creating discrimination liability—even without intent. Implement regular bias audits and maintain human oversight.

☐ **Ensure Employment Law Compliance**

Several jurisdictions require AI disclosure in hiring. The EEOC emphasizes employer liability for AI tool outcomes regardless of vendor involvement.

### 5. ETHICS & ENGAGING EXTERNAL COUNSEL

☐ **Establish Ethical AI Principles**

Define commitments beyond legal compliance addressing fairness, transparency, accountability, and societal impact. Integrate ethics into development and deployment.

## ☐ **Ensure Explainability**

Stakeholders increasingly expect to understand AI decisions. Build explainability into systems and prepare to describe decision-making processes.

### **WHY EXTERNAL COUNSEL IS ESSENTIAL**

The AI legal landscape evolves faster than most internal teams can track. External counsel with specialized AI expertise provides deep specialization in rapidly evolving technology and law, cross-industry perspective on best practices, regulatory relationship insights, objective assessment unaffected by internal pressures, and scalable expertise available when needed.

## ☐ **Engage Counsel Early**

Involve external counsel at the planning stage rather than when problems arise. Early engagement prevents costly mistakes and ensures legal considerations are built into AI strategy.

## ☐ **Build Collaborative Partnership**

The most effective relationships are collaborative partnerships. Share information freely, involve counsel in strategic discussions, and treat them as advisors rather than transactional service providers.

### **TAKE THE NEXT STEP**

Organizations that navigate the AI legal landscape effectively gain competitive advantage. Those that don't face costly mistakes, regulatory penalties, and litigation.

**Don't navigate alone.** This checklist identifies what needs attention—experienced counsel helps you address it.



**Michael S. Baker, P.C.**

*Attorneys & Counselors*

212 Bellvale Lakes Road, Warwick, NY 10990

(212) 203-9234 | [info@nybusiness.law](mailto:info@nybusiness.law)

#### **IMPORTANT DISCLAIMER**

*This checklist is for general educational purposes only and does not constitute legal advice or create an attorney-client relationship. The AI legal landscape is rapidly evolving and varies by jurisdiction. Consult qualified counsel for advice specific to your situation.*

© Michael S. Baker, P.C. All rights reserved.