



pipIQ™: Compliant AI You Can Trust

Why Clients Are Cracking Down on AI Use

Contracts are changing. More companies are inserting strict clauses prohibiting public AI tools like ChatGPT to protect sensitive data. If you're a vendor or partner, using public AI platforms could now violate contracts, void payment terms, or trigger audits.

Common Contract Clauses Now Include:

Do Not Use Public LLMs To Process Client Data

Vendor Must Ensure Data Is Not Used For AI Training.

AI Use Must Be Auditable And Compliant With Internal Policies.

Why It Matters

Using pipIQ can help you:

Maintain trust with clients concerned about AI risk

Confidently sign contracts with AI restrictions

Avoid legal exposure or data breaches

Use AI effectively while staying compliant

How pipIQ™ Solves the Risk

- ✓ **Secure, Private AI Platform**
Unlike public LLM platforms, pipIQ operates in a closed environment. All data stays within your organization's private instance - no external APIs, no third-party data sharing.
- ✓ **No Training On Client Data**
pipIQ never trains its models on your prompts, documents, or usage data. That means your client contracts, proprietary information, and sensitive inputs are fully protected.
- ✓ **Built-In Guardrails And Permissions**
Set custom usage policies, role-based access, and prompt filters. Control how pipIQ is used across your company to meet internal compliance needs and client requirements.
- ✓ **Full Audit Logs**
Set custom usage policies, role-based access, and prompt filters. Control how pipIQ is used across your company to meet internal compliance needs and client requirements.
- ✓ **Document-Aware, Not Document-Exposed**
Employees can upload contracts, NDAs, and SOPs for smarter AI use, but files stay protected within your environment. pipIQ draws insights without risking data leakage.