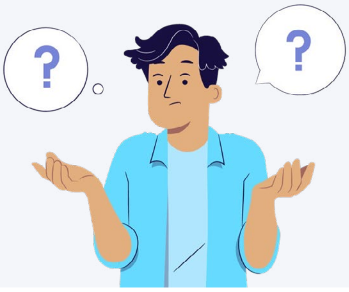
AI Legal Compliance Checklist

If you're planning to roll out a new AI tool or use of AI in your organization, the first step is to check whether it meets legal compliance.

Use the following checklist to gather the necessary details to request support from a legal counsel or data protection officer. They can help you determine whether your application of AI is legally compliant.

Keep in mind

While asking AI tools to process similar requests can point you towards relevant legislation, they **cannot** provide legal advice or certify compliance.



HOW TO USE

Write the answer to each question in a separate document and gather the additional materials listed below. Check off each item as you complete it.

1 AI application and scope

- □ **AI tool/application name**: This could be a résumé screening tool, performance evaluation assistant, employee monitoring software, etc.
- □ **Function/purpose:** Briefly describe what the AI system does in the HR lifecycle (e.g., "Ranks job applicants based on keyword matching," or "Analyzes employee communication data for sentiment.").
- □ **Deployment region:** State the specific geographical regions/jurisdictions where the AI is being used or will be used (e.g., California (CCPA), European Union (GDPR), State of Illinois).

2 Data and processing

- □ **Data type and source:** What kind of personal data does the AI process? (E.g., sensitive data like race/gender, candidate work history, employee communication logs, behavioral data).
- □ **Legal basis for processing:** What is the current assumed legal basis for processing this data? (e.g., Consent, Legitimate Interest, Contractual Necessity). This is crucial for GDPR regions.
- □ **Data storage:** Where is the data physically stored and processed (e.g., local server, US cloud provider, EU cloud provider)?

3 Compliance focus areas

□ **Bias/discrimination check:** Does the organization have an auditable process to test the model for adverse impact or bias against protected characteristics (e.g., age, gender, ethnicity)?

□ **Transparency and explanation:** Is the organization capable of providing an adequate explanation (right to explanation) of how the AI arrived at a specific decision (e.g., why a candidate was rejected)?

□ **Data subject rights:** What processes are in place to manage requests related to the right to access, right to rectification, or right to erasure concerning data processed by the AI?

□ **Notice and consent:** How and when are employees/candidates informed that AI is being used in the process, and is explicit consent obtained where required?

Example question for legal council

"Based on the details above, please conduct a compliance review to identify all legal and regulatory risks (including GDPR, anti-discrimination laws, and specific state/local AI legislation) associated with the deployment of this AI application in our specified regions. Specifically, we need confirmation on the validity of our legal basis for processing and assurance that our [bias testing and transparency procedures] meet statutory requirements."