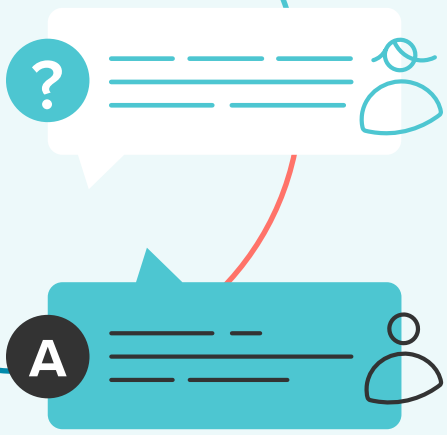
betterworks

Questions for HR AI Software Vendors

If you are considering adopting a generative AI solution as part of your HR tech stack, these questions will help you and your IT and information security teams determine if the solution is secure, compliant, and ethically sound. Understanding data privacy, model training, and vendor practices helps mitigate risks associated with sensitive employee information and prevents potential legal issues. Asking vendors to respond to these questions will help you make an informed decision that aligns with the organization's values and regulatory requirements.

Data Privacy and Security

- Where is our employees' data stored? Is it encrypted both in transit and at rest?
- What security measures are in place to protect employee data from unauthorized access?
- Does your solution comply with relevant data privacy regulations (e.g., GDPR, CCPA)?
- How do you handle data retention and deletion policies, especially concerning generated content?



Model Training and Data Sources:

- Is our employees' data used to train AI models?
- Are you fine-tuning your generative AI models? If yes, what data sources are used to achieve that?
- Are there any steps taken to mitigate bias in the training data and model outputs?
- How do you ensure the model is not generating outputs that could be discriminatory or offensive?
- How frequently are the models updated and retrained?

Algorithm Transparency and Explainability:

- Can you explain how your generative AI models make decisions or create content?
- How do you handle false positives/negatives or errors in AI-generated content?

Vendor Security Practices & Legal Considerations:

- What are your policies regarding third-party access and subcontractors related to generative AI?
- Is your generative AI model based on proprietary technology or a third-party vendor (like OpenAI)?
- How do you ensure compliance with industry-specific regulations concerning generative AI?
- What legal protections and liabilities are in place if the AI system generates harmful or inappropriate content or if breaches occur?