Some Possible Considerations in Choosing an AI Provider for an Organizational Ombuds Office

2026 from AI, with assists from Mary Rowe

Here is a list (from AI) about some concerns that turned up in an early 2026 search that might be of use as you compare AI providers. Consider discussing this list with trusted IT/Legal colleagues. As you read, please consider caveats about information from AI, which may be inadequate, incorrect, or poorly worded here. What follows are some questions to consider as you compare various AI providers.

1. Could sensitive data be inadvertently exposed through strategic questioning posed to the AI?

2. To what extent is information from user interactions logged and retained by the AI provider? This practice raises fears of data being used for training the AI model without users' explicit consent.

3. To what extent is the provider collecting and using extensive data from other services provided by that company?

4. Has the provider faced lawsuits over potential misuse of user data and inadequate privacy protections?

5. Does the provider have certain contractual provisions that may allow human review of confidential prompts?

6. Could broad permissions potentially lead to unauthorized access and data breaches?

7. Have there been reports of the providers' AI agents having or developing unexpected access levels? This could lead to operational and security concerns.

8. Has the provider experienced significant service disruptions? AI-related outages can impact business operations and/or reveal gaps in security handling.

9. Has the provider faced user complaints for overhyping its AI tools' capabilities?

10. How easy or complex is it to manage privacy when using the providers' AI tools?

11. How do the cost and capabilities compare with other providers?

12. Has there been regulatory scrutiny of the provider's data access security?

13. Have there been reports of security flaws and/or privacy risks associated with the provider's AI?

14. Are there reports of user complaints about unresolved issues with subscriptions and/or data handling?

These concerns highlight various challenges and vulnerabilities faced by AI providers in maintaining user privacy and data security. Each provider has some risks, emphasizing the need for stringent privacy protections and user controls.

Overall, one might search for the provider that appears to have earned highest trust about confidentiality.

Using the organizational AI: Pros and cons

Using your employer's AI system involves several considerations regarding security and confidentiality. Here's a breakdown of the pros and cons:

Pros

- **Controlled Environment**:
  - Using an in-house AI system can provide greater control over data handling and security measures. The organization can implement specific security protocols and governance structures to ensure data protection.
- **Customization**:
  - The system can be tailored to meet specific security requirements and business needs, allowing you to address unique confidentiality concerns within your organization.
- **Data Privacy**:
  - If the data do not leave the organization, there is reduced risk of exposure to external threats. The AI system can be designed to comply with internal policies and regulatory standards.
- **Integration with Existing Security**:
  - Leveraging existing security infrastructure can enhance protection, utilizing familiar protocols and practices that align with company policies.

Cons

- **Insider Threats**:
  - Employees with access to the AI system might misuse information. Ensuring robust access controls and monitoring is crucial to mitigate this risk.
- **Resource Intensive**:
  - Maintaining a secure AI system requires significant investment in security measures, regular audits, and continuous monitoring, which can strain organizational resources.
- **Complexity in Management**:
  - Managing and updating security measures in-house can be complex and requires constant vigilance to adapt to emerging threats.
- **Limited Expertise**:
  - In-house systems might lack the advanced security features and expertise that specialized AI providers offer, potentially leaving the organization vulnerable to sophisticated attacks.

Summary

Using your employer's AI can provide greater control and customization over security measures, which is beneficial for internal data protection. However, it demands substantial investment by the employer and poses risks from insider threats and management complexities. Regular audits, strong access controls, and ongoing education about potential vulnerabilities can help enhance security and confidentiality.

Note: AI may present inaccurate, insufficient or offensive responses.

This article draft is part of a Resource Repository designed to support identifying—and helping to quantify—the value of an Organizational Ombuds (OO). This Resource Repository is a work in progress. It is open to improvements, additions, deletions, critique, revision and random commentary. If any page in the repository is helpful, or needs revision, please let us know. Please contact Mary Rowe or other co-authors, if you can help to improve these pages or have another page to offer.