

CHECKLIST

Addressing Data Privacy in Ai-based Knowledge Management

Securing AI knowledge management systems

- 1 Deploy automated access controls like Okta at every data ingestion point immediately.
- 2 Implement real-time consent dashboards to make permission withdrawal as easy as opt-in.
- 3 Audit your AI vendor's encryption, data residency, and GDPR compliance line-by-line.
- 4 Run quarterly data pruning audits to minimize what your AI system actually needs.
- 5 Set maximum data retention at 12 months for sensitive files using auto-purging.
- 6 Enforce monthly privacy training for all employees using services like KnowBe4.
- 7 Conduct quarterly permission reviews and establish real consequences for access lapses.
- 8 Subscribe to a regulatory monitoring service like TrustArc for real-time compliance updates.
- 9 Document who has access to what data and revoke all legacy permissions.
- 10 Never rely on static consent forms; require dynamic, user-controlled permissions always.
- 11 Audit your knowledge base for accidental sensitive data uploads monthly.

Read the full article: <https://nlobrain.com/blog/addressing-data-privacy-in-ai-based-knowledge-management/>

nlobrain.com