DEKODIERT TOOL RADAR

Agentic Memory Vendor Radar for DE/EU

A due-diligence map for company memory in agentic AI systems.

Public-source status: 2026-05-17

> No legal advice. No purchase recommendation. Vendor statements are not independent audits.

Memory layers

KÜRZEL	SCHICHT	WORUM ES GEHT
RET	Retrieval / Enterprise Search	Finding knowledge in documents, tickets, email, wikis, and apps
DOC	Document structure	OCR, parsing, tables, layout, clauses, extraction
REL	Relationships / Knowledge Graph	Customers, cases, products, contracts, risks, processes, and their relationships
FLOW	Work traces / Evals	Prompts, tool calls, feedback, approvals, evaluations, agent runs
MULTI	Multimodal	Images, screenshots, technical drawings, video, audio
ORCH	Orchestration / Agent Runtime	Agents, permissions, actions, guardrails, human approval

Vendor cards

Work-AI Platform

Microsoft

primary-source

Microsoft 365 Copilot / Copilot Studio

RET FLOW ORCH DOC-partial REL-via-Graph

Primary fit: M365 default work context, Microsoft Graph, Copilot activity history, agents

DE/EU reading: Strong for existing M365 governance, but high default lock-in risk; Anthropic models out of EU Data Boundary per Microsoft page

Portability: Exports exist for some activity history, but semantic portability of agent memory/evals/workflows unclear

Public privacy/security: GDPR; EU Data Boundary; no foundation model training on prompts/responses/Graph data; Purview retention/search; Teams Export APIs

Maturity: 4 | **Works council:** high | **Overall risk:** medium

Open checks: Copilot Studio agent traces; export of agent memory; subprocessor details; Betriebsrat implications for user activity history

Sources

- https://learn.microsoft.com/en-us/microsoft-365/copilot/microsoft-365-copilot-privacy

Google

primary-source

Google Gemini Enterprise

RET DOC-partial FLOW ORCH MULTI

Primary fit: Workspace and cross-suite enterprise AI, agents, connectors, NotebookLM Enterprise

DE/EU reading: Interesting if Google Cloud governance is strong; less natural default in M365-heavy DE companies

Portability: Portability of agents, indexed data, traces and memories unclear

Public privacy/security: Data security and sovereignty features claimed; compliance examples HIPAA/FedRAMP; details edition-dependent

Maturity: 3	**Works council:** medium-high	**Overall risk:** medium

Open checks: DPA/subprocessors; exact EU residency; export of agent designer logs; connector data handling

Sources

- https://cloud.google.com/gemini-enterprise

Glean

primary-source

Glean Work AI Platform

RET REL FLOW ORCH

Primary fit: Enterprise search, Enterprise Graph, Personal Graph, Work AI agents

DE/EU reading: Strong platform, strong lock-in potential; relevant where enterprise search is strategic

Portability: Portability of Enterprise Graph, Personal Graph, agent traces and feedback unclear

Public privacy/security: SOC/GDPR/HIPAA claims; single-tenant; enforced permissions; zero-retention model provider agreements; sensitive-content policies

Maturity: 4	**Works council:** high	**Overall risk:** medium-high

Open checks: Trust Center details; DPA; subprocessor list; export semantics for graphs and personal context

Sources

- https://www.glean.com/
- https://www.glean.com/security

Sovereign AI / RAG / IDP / Agents

deepset

primary-source

Haystack / Haystack Enterprise Platform

RET DOC ORCH MULTI REL-partial FLOW-partial

Primary fit: Controlled RAG, IDP, agents, Text-to-SQL, open-source foundation

DE/EU reading: Strong DE/EU candidate due sovereignty positioning and deployment flexibility

Portability: High potential portability via open-source Haystack and modular architecture, but project-specific

Public privacy/security: SOC 2 Type II; ISO 27001; GDPR; HIPAA; CSA Star Level 1 claimed

Maturity: 4	**Works council:** medium	**Overall risk:** low-medium

Open checks: Detailed enterprise DPA/subprocessors; export of platform configs/evals/traces; concrete EU hosting commitments

Sources

- https://www.deepset.ai/

LLM Observability / Evals

Langfuse

primary-source

Langfuse

FLOW

Primary fit: Tracing, prompt management, evaluation, metrics, audit, retention/masking/deletion

DE/EU reading: Very strong DE/EU control layer, especially self-hosted or EU region

Portability: Good due OSS/self-hosting; trace/eval export still needs technical validation

Public privacy/security: SOC 2 Type II; ISO 27001; GDPR; DPA; EU region eu-west-1; data retention/masking/deletion

Maturity: 4	**Works council:** high if personenbezogene traces	**Overall risk:** low-medium

Open checks: Exact export formats; enterprise audit logs; Betriebsrat template for traces and feedback

Sources

- https://langfuse.com/security

Braintrust

primary-source

Braintrust

FLOW

Primary fit: Tracing, evals, prompts, scorers, human review, datasets, exports

DE/EU reading: Strong option where traces/evals must remain in customer cloud/region; control plane metadata and telemetry still require review

Portability: Docs include exports, datasets, API/SDK/CLI and self-hosted data plane; exact export formats still need technical validation

Public privacy/security: Self-hosting docs separate sensitive AI data in customer-controlled data plane; data plane stores experiment records, logs, traces, spans, datasets, prompt completions, human review scores and provider secrets; control plane stores metadata/login/org info; telemetry can be sent back for health/billing/support

Maturity: 3	**Works council:** high if personenbezogene traces	**Overall risk:** low-medium

Open checks: DPA/subprocessor/public security reports; EU fully hosted region; telemetry defaults; export formats; remote access procedures

Sources

- https://www.braintrust.dev/docs
- https://www.braintrust.dev/docs/admin/self-hosting

Arize

primary-source

Arize Phoenix / AX

FLOW

Primary fit: Phoenix OSS, evals, observability, AI agent reliability

DE/EU reading: Phoenix OSS/self-hosting is a strong control pattern for DE/EU traces; Arize AX/Phoenix Cloud enterprise terms still need trust/legal review

Portability: OSS/OpenInference/OpenTelemetry orientation improves control; cloud export and enterprise retention need validation

Public privacy/security: Phoenix docs expose self-hosting, RBAC, API keys, secrets, data retention and security/privacy/network security sections; cloud/security claims not deeply fetched

Maturity: 3	**Works council:** high if personenbezogene traces	**Overall risk:** low-medium for self-hosted Phoenix; medium for cloud

Open checks: Arize AX Trust/Security/DPA; EU region; subprocessors; cloud retention; enterprise support terms

Sources

- https://arize.com/phoenix/
- https://arize.com/docs/phoenix
- https://arize.com/docs/phoenix/self-hosting
- https://arize.com/docs/phoenix/settings/data-retention
- https://arize.com/docs/phoenix/settings/access-control-rbac

Galileo

docs-claim

Galileo

FLOW

Primary fit: AI observability, evals, agent reliability, Protect

DE/EU reading: Functionally relevant observability/evals layer; public docs showed security navigation but detailed security pages returned 404 in this pass

Portability: Unknown

Public privacy/security: Docs cover tracing, sessions, multimodal observability, distributed tracing, OpenTelemetry, evals, runtime protection, annotations, projects, access control and SSO in navigation; security details not publicly verified

Maturity: 2	**Works council:** high if personenbezogene traces	**Overall risk:** medium-high

Open checks: Correct security docs; DPA; EU region; subprocessors; self-host/BYOC; export; retention; access-control docs fetchable URL

Sources

- https://docs.galileo.ai/what-is-galileo
- https://docs.galileo.ai/security/access-control
- https://docs.galileo.ai/security/sso-integration

LLM Observability / Evals / Agent Platform

LangChain

primary-source

LangSmith

FLOW ORCH

Primary fit: Agent tracing, evals, monitoring, deployment, SmithDB

DE/EU reading: Powerful but DE/EU depends heavily on BYOC/self-hosting; US cloud otherwise sensitive

Portability: Self-host/BYOC improves control; portability of traces/evals needs review

Public privacy/security: HIPAA; SOC 2 Type 2; GDPR claimed; Trust Center referenced

Maturity: 3	**Works council:** high if cloud with personenbezogene traces	**Overall risk:** medium

Open checks: EU region availability; DPA; subprocessor; export formats; self-host contractual model

Sources

- https://www.langchain.com/langsmith/observability
- https://docs.langchain.com/langsmith/home

Search / Observability / Context Engineering

Elastic

primary-source

Elasticsearch / Elastic AI

RET FLOW ORCH-partial MULTI-partial

Primary fit: Open search, hybrid retrieval, logs, workflows, model-agnostic AI stack

DE/EU reading: Strong infrastructure candidate where existing Elastic skills exist; not a complete memory solution

Portability: Strong data ownership if self-managed; product-specific agent artifacts need review

Public privacy/security: Security/compliance not fully captured in this pass; open/self-managed architecture relevant

Maturity: 4	**Works council:** medium	**Overall risk:** low-medium

Open checks: Exact licensing; cloud region; agent builder data; export of workflows and traces

Sources

- https://www.elastic.co/security

Vector DB / Hybrid Search

Weaviate

primary-source

Weaviate Cloud / Weaviate Agents

RET ORCH-partial

Primary fit: Vector/hybrid search, RAG, agentic AI, dedicated cloud/BYOC

DE/EU reading: EU-based vendor; good retrieval building block, not full memory

Portability: Index/data export and schema portability need technical validation

Public privacy/security: SOC 2; HIPAA; privacy; encryption; RBAC; multi-tenancy; backups claimed

Maturity: 3	**Works council:** medium	**Overall risk:** low-medium

Open checks: DPA/subprocessors; EU region; agent products maturity; export semantics

Sources

- https://weaviate.io/security

Vector DB

Pinecone

primary-source

Pinecone Vector Database

RET

Primary fit: Vector database for RAG and semantic retrieval

DE/EU reading: Strong vector component; US vendor; not full memory

Portability: Portability of embeddings/index metadata must be designed by customer

Public privacy/security: SOC 2 Type II; HIPAA; GDPR-ready; encryption; audit logs

Maturity: 3	**Works council:** medium	**Overall risk:** medium

Open checks: EU region specifics; DPA/subprocessors; export/rebuild process for indexes

Sources

- https://www.pinecone.io/security/

Qdrant

primary-source

Qdrant Vector Database

RET

Primary fit: Vector database, RAG, recommendation, agentic use cases

DE/EU reading: Strong control story for Hybrid/Private Cloud because customer controls infrastructure and storage; Managed Cloud still needs region/subprocessor review

Portability: Better than many SaaS-only vector stores if self-hosted or private cloud; export/rebuild of collections, payloads and vectors still project-owned validation

Public privacy/security: SOC 2 Type 2 and HIPAA stated; Trust Center; encryption at rest/in transit; RBAC; SSO for Premium; DPA offered for GDPR customers; API keys not stored in plaintext; SBOM and signed images for Hybrid/Private Cloud

Maturity: 3	**Works council:** medium	**Overall risk:** low-medium

Open checks: Managed Cloud EU regions and subprocessors; concrete DPA terms; collection export/rebuild procedure; inference feature data handling

Sources

- https://qdrant.tech/documentation/cloud-security/

Knowledge Graph

Neo4j

primary-source

Neo4j Graph Database / Aura Agent

REL | RET-via-GraphRAG | ORCH-partial

Primary fit: Knowledge graphs, graph database, GraphRAG, relationships

DE/EU reading: Strong for relationship memory; good candidate if graph is explicit asset

Portability: Graph export possible in principle, but app semantics and Aura Agent artifacts need review

Public privacy/security: Security team; Trust Center; subprocessor list referenced; details not fully fetched

Maturity: 4	**Works council:** medium	**Overall risk:** low-medium

Open checks: Aura regions; DPA/subprocessors; Aura Agent logs/export; EU deployment specifics

Sources

- https://neo4j.com/security/

Knowledge Graph / Semantic AI

Graphwise

primary-source

Ontotext GraphDB

REL | RET | DOC-partial

Primary fit: RDF/SPARQL knowledge graph, semantic metadata, GraphRAG, MCP support

DE/EU reading: Very strong for explicit semantics and standards, good DE/EU fit to investigate

Portability: Strong standards portability if modeled well; implementation complexity high

Public privacy/security: Security details not fully assessed; W3C standards reduce semantic lock-in

Maturity: 4	**Works council:** medium	**Overall risk:** low-medium

Open checks: Contract/security docs; EU hosting; DPA/subprocessors; managed-service terms

Sources

- https://www.ontotext.com/products/graphdb/

Semantic AI / Taxonomy / Knowledge Graph

Graphwise

primary-source

PoolParty Semantic Suite

REL DOC RET

Primary fit: Taxonomies, ontologies, semantic search, GraphRAG, SharePoint integration

DE/EU reading: Strong DE/EU candidate; EU company; ISO 27001/27701 claims

Portability: Good semantic portability if taxonomies/ontologies owned by customer

Public privacy/security: ISO/IEC 27001:2022 and ISO/IEC 27701:2019; Keycloak; EU-based

Maturity: 4	**Works council:** medium	**Overall risk:** low-medium

Open checks: Deployment models; DPA; subprocessor; export of taxonomies/ontologies/config

Sources

- https://www.poolparty.biz/

Document Processing / IDP

Unstructured

vendor-claim

Unstructured Data Platform

DOC RET-support

Primary fit: Parse, chunk, embed, enrich, ETL for unstructured files

DE/EU reading: Useful document pipeline, but public security URL returned 404; not enough for low-risk DE/EU claim

Portability: Structured outputs/pipelines are the portability object; exact export formats, connector state and enrichment artifacts need validation

Public privacy/security: Homepage/product pages claim security and compliance built in and role-based access; Trust Portal mentioned in first pass, but security page fetch returned 404

Maturity: 3	**Works council:** medium	**Overall risk:** medium-high

Open checks: Trust Portal; DPA; EU region; subprocessors; retention; self-host/private deployment; export formats; connector state portability

Sources

- https://unstructured.io/
- https://unstructured.io/product
- https://unstructured.io/security

Document Agents / Framework

LlamaIndex

vendor-claim

LlamaParse / LlamaIndex

DOC RET ORCH-partial

Primary fit: Document parsing, extraction, indexing, workflows, developer framework

DE/EU reading: Functionally strong document-agent layer; public security/legal evidence is thinner than enterprise positioning, so not a low-risk DE/EU default

Portability: OSS framework improves architecture portability; SaaS parsing outputs and retention/data handling must be verified before sensitive documents

Public privacy/security: Homepage claims granular access controls, enhanced encryption, HIPAA, GDPR and SOC2; footer exposes Trust Center, Privacy Notice, Terms and DPA links, but direct DPA/privacy/security fetch returned 404 in this pass

Maturity: 3	**Works council:** medium	**Overall risk:** medium-high

Open checks: Correct Trust Center/DPA/Privacy URLs; retention; EU region; subprocessors; VPC terms; export of parse/extract/index artifacts

Sources

- https://www.llamaindex.ai/
- https://www.llamaindex.ai/llamacloud
- https://www.llamaindex.ai/data-processing-addendum

Agent Memory / Temporal Graph

Zep

primary-source

Zep / Graphiti

FLOW REL RET

Primary fit: Agent memory, temporal knowledge graph, context engineering, facts/entities/episodes

DE/EU reading: Conceptually central for agent memory, but public enterprise security and regional evidence were not found in this pass; use as emerging layer, not as low-risk enterprise recommendation

Portability: Graphiti OSS and explicit graph primitives are promising; hosted Zep export semantics and deletion controls need validation

Public privacy/security: Docs describe context graphs, user graphs, threads, facts, entities, episodes, fact invalidation and Graphiti OSS; no public security/DPA/EU-region evidence captured

Maturity: 2	**Works council:** high if user-specific memory	**Overall risk:** medium-high

Open checks: Security, DPA, EU region, self-hosting, deletion of user-specific memories, export semantics, subprocessors

Sources

- https://help.getzep.com/
- https://help.getzep.com/llms-full.txt

Agent Memory

Mem0

trust-center-gated

Mem0

FLOW REL-partial

Primary fit: Persistent memory infrastructure for agents, memory compression, audit logs

DE/EU reading: Relevant memory layer, but Trust Center was blocked by Vercel 429 and privacy URL returned 404; do not present as fully verified for DE/EU

Portability: Same API across Kubernetes/private cloud/air-gapped is claimed; actual memory export format and semantic portability unverified

Public privacy/security: Homepage claims SOC 2 Type 1, HIPAA, BYOK, zero-trust, governance, audit logs; Enterprise pricing lists audit logs and SSO

Maturity: 2	**Works council:** high if personenbezogene memory	**Overall risk:** medium-high

Open checks: Trust Center access; privacy policy URL; DPA; EU region; subprocessors; SOC2 Type2; memory export/deletion; personenbezogene memories

Sources

- https://mem0.ai/
- https://mem0.ai/pricing
- https://trust.mem0.ai/
- https://mem0.ai/privacy

Memory-first agents

Letta

primary-source

Letta / Letta Code

FLOW ORCH

Primary fit: Persistent agents, continual learning, model-portable memory, git-based context repositories

DE/EU reading: Technically important emerging memory-first agent concept; public enterprise compliance evidence not found; should be framed as frontier signal, not procurement candidate

Portability: Model-portable memories and git-based context repositories are promising, but enterprise export/audit semantics are unverified

Public privacy/security: Public site covers memory-first agents, portability across models, local/remote/device claims, git-based context repositories; no enterprise security/DPA/region evidence captured

Maturity: 1	**Works council:** high if deployed broadly	**Overall risk:** unknown

Open checks: Enterprise security, DPA, data flow, hosting, audit, export, deletion, customer-controlled deployment

Sources

- https://www.letta.com/

Agent Runtime / Memory

Anthropic

vendor-claim

Managed Agents / Memory / Dreams

FLOW ORCH

Primary fit: Managed agents, memory stores, dreams, evals, traces

DE/EU reading: High strategic relevance, but vendor-controlled memory/orchestration is the risk case

Portability: Memory stores/evals/traces portability unclear

Public privacy/security: Security/privacy to assess via Anthropic docs; Microsoft notes Anthropic subprocessor out of EU Data Boundary in Copilot context

Maturity: 2	**Works council:** high	**Overall risk:** medium-high

Open checks: Enterprise availability; DPA; EU processing; memory export; eval portability; subprocessor

Sources

- https://claude.com/blog/claude-managed-agents
- https://platform.claude.com/docs/en/managed-agents/dreams
- https://www.anthropic.com/engineering/demystifying-evals-for-ai-agents

Cloud Document AI

Azure

primary-source

Azure AI Document Intelligence

DOC MULTI-partial

Primary fit: Document extraction, OCR, structured document AI

DE/EU reading: Relevant for document structure in Microsoft/Azure shops

Portability: Export structured outputs likely; pipeline ownership customer-dependent

Public privacy/security: Needs source pass

Maturity: 3	**Works council:** medium	**Overall risk:** medium

Open checks: Fetch product/security docs, data residency, DPA, model training, retention

Sources

- https://learn.microsoft.com/en-us/azure/ai-services/document-intelligence/overview

Google

primary-source

Google Document AI

DOC MULTI-partial

Primary fit: Document extraction and parsing

DE/EU reading: Relevant if Google Cloud already governed

Portability: Pipeline outputs exportable, model/data handling to verify

Public privacy/security: Needs source pass

Maturity: 3	**Works council:** medium	**Overall risk:** medium

Open checks: Fetch product/security docs, data residency, DPA, training, retention

Sources

- https://cloud.google.com/document-ai/docs/overview

Cloud Document AI / RAG

AWS

primary-source

AWS Textract / Bedrock Knowledge Bases

DOC RET MULTI-partial

Primary fit: Document extraction, managed RAG in AWS ecosystem

DE/EU reading: Relevant for AWS-heavy firms and regulated workloads

Portability: Customer controls depend architecture; managed service lock-in possible

Public privacy/security: Needs source pass

Maturity: 3	**Works council:** medium	**Overall risk:** medium

Open checks: Fetch product/security docs, data residency, DPA, training, retention

Sources

- https://aws.amazon.com/textract/
- https://aws.amazon.com/bedrock/knowledge-bases/

Work-AI / CRM Agent Platform

Salesforce

primary-source

Agentforce

REL FLOW ORCH RET-partial

Primary fit: CRM-centered autonomous agents, Salesforce data/process context, Slack and Customer 360 ecosystem

DE/EU reading: Must be in scope for any enterprise vendor radar because Salesforce owns critical customer/process context; DE/EU readiness depends on Salesforce contractual setup, Hyperforce/data residency and subprocessors

Portability: High business-process lock-in risk if agent logic, feedback and CRM context remain inside Salesforce ecosystem

Public privacy/security: Product page covers build/deploy/manage agents at scale and integration with Salesforce ecosystem; security/privacy details not deeply fetched in this pass

Maturity: 4	**Works council:** high if agents affect sales/service performance or employee workflows	**Overall risk:** medium-high

Open checks: Trust/DPA/subprocessors; EU data residency; Agentforce traces; agent export; Data 360 semantics; Slack interaction data

Sources

- https://www.salesforce.com/agentforce/

Work-AI / Workflow Platform

ServiceNow

primary-source

ServiceNow AI Agents

FLOW ORCH REL RET-partial

Primary fit: Workflow automation, IT/HR/CRM/service operations, AI Control Tower and process context

DE/EU reading: Important enterprise workflow layer; high relevance where ServiceNow is the system of work for IT/HR/service. Treat as process-memory platform, not just AI feature

Portability: Process and workflow context can become deep platform dependency; export of agent configs/traces/control tower data needs validation

Public privacy/security: Product page states AI/data/workflows on one platform, AI agents assigned to roles with business context and permissions; Responsible AI and security platform references; detailed trust/legal not fetched

Maturity: 4	**Works council:** high if workflows, employee service, IT performance or process mining are involved	**Overall risk:** medium-high

Open checks: Trust/DPA/subprocessors; EU region; AI Control Tower data model; agent trace export; process mining personenbezogene Daten

Sources

- https://www.servicenow.com/products/ai-agents.html

Work-AI / Teamwork Platform

Atlassian

primary-source

Rovo

RET REL FLOW ORCH

Primary fit: Teamwork Graph, enterprise search, chat, agents, Jira/Confluence/Loom context and connected SaaS apps

DE/EU reading: Strong collaboration-memory candidate in Atlassian-heavy organizations; cloud dependency and graph/context portability are key risks

Portability: Teamwork Graph and connected context are likely hard to migrate semantically; export of agents/search graph/traces unclear

Public privacy/security: Rovo page states admin controls, AI deactivation, SOC 2 and ISO 27001 assessment/certifications, restrictive LLM provider policies and subprocessor page reference

Maturity: 4	**Works council:** high if agent actions, productivity flows or collaboration analytics touch employees	**Overall risk:** medium

Open checks: AI subprocessor details; EU data residency; graph export; Rovo agent logs; connector data handling; retention

Sources

- https://www.atlassian.com/software/rovo

Work-AI / ERP Process Platform

SAP

primary-source

Joule / Joule Agents / SAP Business AI Platform

REL FLOW ORCH RET DOC-partial

Primary fit: SAP process context, SAP Knowledge Graph, Business Data Cloud, Joule assistants/agents across business functions

DE/EU reading: Central for SAP-heavy enterprises because process memory sits near ERP/HCM/procurement/finance; useful in article because it proves the thesis from inside SAP, not outside

Portability: High semantic lock-in risk if process context, SAP Knowledge Graph grounding and agent workflows remain SAP-internal

Public privacy/security: SAP page states GDPR compliance, tenant-level data isolation, no customer data stored within Joule, data masking/pseudonymization, SAP global data protection policy

Maturity: 4	**Works council:** high in HR, finance, procurement and workflow automation contexts	**Overall risk:** medium

Open checks: DPA/subprocessors; exact Joule data retention; agent trace export; SAP Knowledge Graph portability; non-SAP connector handling

Sources

- https://www.sap.com/products/artificial-intelligence.html

Work-AI / HCM-Finance Platform

Workday

primary-source

Workday AI / Sana / Agents / Agent System of Record

REL FLOW ORCH RET-partial

Primary fit: HCM, finance and work graph/agent system in Workday context

DE/EU reading: Potentially high DE/EU relevance because HCM/employee data is sensitive; must be treated as high-governance workflow memory

Portability: High lock-in risk where employee, finance and agent-system records sit in Workday

Public privacy/security: Public AI page fetched; detailed trust/legal/security claims not extracted in this pass

Maturity: 3	**Works council:** high due HCM/ employee-work context	**Overall risk:** medium-high

Open checks: Trust/DPA/subprocessors; EU residency; Agent System of Record export; employee data traces; retention; works council implications

Sources

- https://www.workday.com/en-us/artificial-intelligence.html

Work-AI / Knowledge Workspace

Notion

primary-source

Notion AI / Agents / Enterprise Search

RET FLOW ORCH DOC-partial

Primary fit: Workspace-native AI, enterprise search, custom agents, meeting notes, connected apps

DE/EU reading: Relevant for knowledge-work teams but less core-enterprise than M365/Google/Atlassian; treat as workspace memory with connector and retention risk

Portability: Notion pages/databases export separately from AI agents, custom agents, search index and meeting memory; semantic portability unclear

Public privacy/security: Product page states no training on customer data via AI subprocessors, SOC 2 Type 2, ISO 27001, GDPR/CCPA mapped privacy program, TLS encryption, zero data retention with LLM providers for Enterprise and 30 days for non-Enterprise, HIPAA for Enterprise

Maturity: 3	**Works council:** medium-high if meeting notes, agents and search expose employee work patterns	**Overall risk:** medium

Open checks: AI subprocessor list; EU residency; custom agent export; meeting transcript retention; enterprise search index portability

Sources

- https://www.notion.com/product/ai

AI Production Platform / Agent Runtime

Mistral AI

primary-source

Mistral AI Studio

FLOW ORCH RET REL-partial

Primary fit: Agent runtime, observability, AI registry, evals, datasets, workflow telemetry, deployable AI production platform

DE/EU reading: Strong DE/EU candidate to watch because deployable-anywhere, self-hosting and European vendor context align with sovereignty needs; still needs trust/legal review

Portability: Page explicitly claims exportable artifacts and unified registry/version control; technical validation still needed

Public privacy/security: Product page states privacy by design, full data ownership, state/telemetry control, self-hosting, dedicated environments, data governance, auditability and DPA link in footer

Maturity: 3

Works council: high if traces/workflow telemetry contain personenbezogene work data

Overall risk: low-medium

Open checks: DPA/subprocessors; enterprise security certifications; EU/on-prem terms; export formats; trace retention; audit log access

Sources

- https://mistral.ai/products/studio

Tabular appendix

VENDOR	STACK	LAYER	RISK	CLAIM	OPEN CHECKS
Microsoft	Microsoft 365 Copilot / Copilot Studio	RET;FLOW;ORCH;DOC-partial;REL-via-Graph	medium	primary-source	Copilot Studio agent traces; export of agent memory; subprocessor details; Betriebsrat implications for user activity history
Google	Google Gemini Enterprise	RET;DOC-partial;FLOW;ORCH;MULTI	medium	primary-source	DPA/subprocessors; exact EU residency; export of agent designer logs; connector data handling
Glean	Glean Work AI Platform	RET;REL;FLOW;ORCH	medium-high	primary-source	Trust Center details; DPA; subprocessor list; export semantics for graphs and personal context
deepset	Haystack / Haystack Enterprise Platform	RET;DOC;ORCH;MULTI;REL-partial;FLOW-partial	low-medium	primary-source	Detailed enterprise DPA/subprocessors; export of platform configs/evals/traces; concrete EU hosting commitments
Langfuse	Langfuse	FLOW	low-medium	primary-source	Exact export formats; enterprise audit logs; Betriebsrat template for traces and feedback
LangChain	LangSmith	FLOW;ORCH	medium	primary-source	EU region availability; DPA; subprocessor; export formats; self-host contractual model
Elastic	Elasticsearch / Elastic AI	RET;FLOW;ORCH-partial;MULTI-partial	low-medium	primary-source	Exact licensing; cloud region; agent builder data; export of workflows and traces
Weaviate	Weaviate Cloud / Weaviate Agents	RET;ORCH-partial	low-medium	primary-source	DPA/subprocessors; EU region; agent products maturity; export semantics
Pinecone	Pinecone Vector Database	RET	medium	primary-source	EU region specifics; DPA/subprocessors; export/rebuild process for indexes
Qdrant	Qdrant Vector Database	RET	low-medium	primary-source	Managed Cloud EU regions and subprocessors; concrete DPA terms; collection export/rebuild procedure; inference feature data handling
Neo4j	Neo4j Graph Database / Aura Agent	REL;RET-via-GraphRAG;ORCH-partial	low-medium	primary-source	Aura regions; DPA/subprocessors; Aura Agent logs/export; EU deployment specifics
Graphwise	Ontotext GraphDB	REL;RET;DOC-partial	low-medium		

VENDOR	STACK	LAYER	RISK	CLAIM	OPEN CHECKS
				primary-source	Contract/security docs; EU hosting; DPA/subprocessors; managed-service terms
Graphwise	PoolParty Semantic Suite	REL;DOC;RET	low-medium	primary-source	Deployment models; DPA; subprocessor; export of taxonomies/ontologies/config
Unstructured	Unstructured Data Platform	DOC;RET-support	medium-high	vendor-claim	Trust Portal; DPA; EU region; subprocessors; retention; self-host/private deployment; export formats; connector state portability
LlamaIndex	LlamaParse / LlamaIndex	DOC;RET;ORCH-partial	medium-high	vendor-claim	Correct Trust Center/DPA/Privacy URLs; retention; EU region; subprocessors; VPC terms; export of parse/extract/index artifacts
Zep	Zep / Graphiti	FLOW;REL;RET	medium-high	primary-source	Security, DPA, EU region, self-hosting, deletion of user-specific memories, export semantics, subprocessors
Mem0	Mem0	FLOW;REL-partial	medium-high	trust-center-gated	Trust Center access; privacy policy URL; DPA; EU region; subprocessors; SOC2 Type2; memory export/deletion; personenbezogene memories
Letta	Letta / Letta Code	FLOW;ORCH	unknown	primary-source	Enterprise security, DPA, data flow, hosting, audit, export, deletion, customer-controlled deployment
Braintrust	Braintrust	FLOW	low-medium	primary-source	DPA/subprocessor/public security reports; EU fully hosted region; telemetry defaults; export formats; remote access procedures
Arize	Arize Phoenix / AX	FLOW	low-medium for self-hosted Phoenix; medium for cloud	primary-source	Arize AX Trust/Security/DPA; EU region; subprocessors; cloud retention; enterprise support terms
Galileo	Galileo	FLOW	medium-high	docs-claim	Correct security docs; DPA; EU region; subprocessors; self-host/BYOC; export; retention; access-control docs fetchable URL
Anthropic	Managed Agents / Memory / Dreams	FLOW;ORCH	medium-high	vendor-claim	Enterprise availability; DPA; EU processing; memory export; eval portability; subprocessor
Azure	Azure AI Document Intelligence	DOC;MULTI-partial	medium	primary-source	Fetch product/security docs, data residency, DPA, model training, retention
Google	Google Document AI	DOC;MULTI-partial	medium	primary-source	Fetch product/security docs, data residency, DPA, training, retention
AWS	AWS Textract / Bedrock Knowledge Bases	DOC;RET;MULTI-partial	medium	primary-source	Fetch product/security docs, data residency, DPA, training, retention
Salesforce	Agentforce	REL;FLOW;ORCH;RET-partial	medium-high	primary-source	Trust/DPA/subprocessors; EU data residency; Agentforce traces; agent export; Data 360 semantics; Slack interaction data
ServiceNow	ServiceNow AI Agents	FLOW;ORCH;REL;RET-partial	medium-high	primary-source	Trust/DPA/subprocessors; EU region; AI Control Tower data model; agent trace export; process mining personenbezogene Daten
Atlassian	Rovo	RET;REL;FLOW;ORCH	medium	primary-source	AI subprocessor details; EU data residency; graph export; Rovo agent logs; connector data handling; retention
SAP	Joule / Joule Agents / SAP Business AI Platform	REL;FLOW;ORCH;RET; DOC-partial	medium	primary-source	DPA/subprocessors; exact Joule data retention; agent trace export; SAP Knowledge Graph portability; non-SAP connector handling
Workday	Workday AI / Sana / Agents / Agent System of Record	REL;FLOW;ORCH;RET-partial	medium-high	primary-source	Trust/DPA/subprocessors; EU residency; Agent System of Record export; employee data traces; retention; works council implications
Notion	Notion AI / Agents / Enterprise Search	RET;FLOW;ORCH;DOC-partial	medium	primary-source	AI subprocessor list; EU residency; custom agent export; meeting transcript retention; enterprise search index portability
Mistral AI	Mistral AI Studio	FLOW;ORCH;RET;REL-partial	low-medium	primary-source	DPA/subprocessors; enterprise security certifications; EU/on-prem terms; export formats; trace retention; audit log access