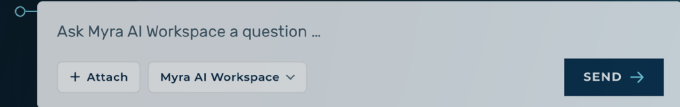




— MYRA AI WORKSPACE **NEW**

**One platform.
20+ AI providers.
100% data protection.**

The sovereign AI platform for organizations
with sensitive data



AI for European organizations with sensitive data

The pilot phase is over: generative AI has long become part of daily operations for many organizations. For an organization-wide rollout, however, clear rules for compliance, cost, and security are often missing.

Myra AI Workspace addresses this with a central, secure work environment for your entire organization. The solution gives your employees access to leading AI models through a familiar chat interface, while you retain control over data flows, budgets, and usage.



What blocks AI rollouts



Shadow AI at work: 41% use private accounts for work tasks.

MYRA SECURITY 2026



1 in 2 employees has held back from using AI due to data privacy and compliance concerns.

MYRA SECURITY 2026



Only 35% of companies have transparent visibility into their AI costs.

KPMG 2026



39% are concerned that company data could end up in the wrong hands.

BITKOM 2026

What Myra offers instead

- One familiar interface for 20+ AI providers
- Sensitive data protected on Myra's own certified EU infrastructure
- Audit-ready with GDPR-compliant logging and guardrails
- No vendor lock-in: switch models at any time
- Predictable costs with budgets for organization, team, and user
- Security proven for critical infrastructure since 2012

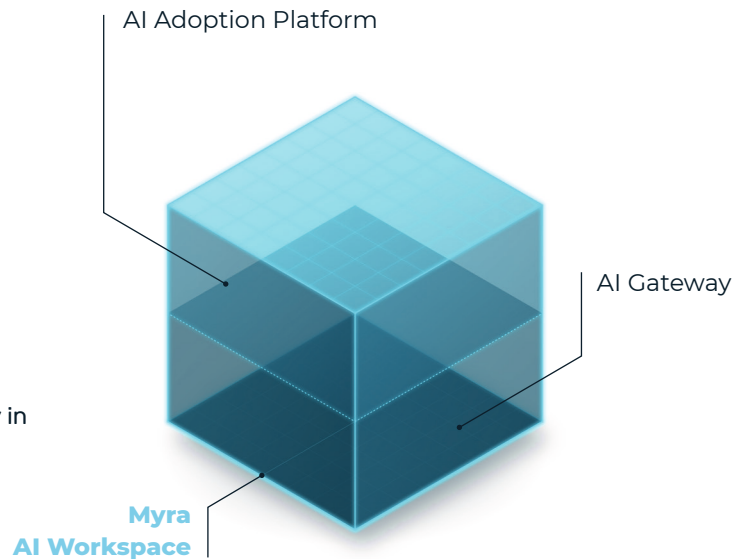
— THE SOLUTION

What is Myra AI Workspace?

The best of both worlds

Myra AI Workspace combines the governance of an AI Gateway with the usability of an intuitive AI Adoption Platform in a single, central solution.

- No parallel setup of a gateway layer and a separate chat application
- Governance that does not cost usability – guardrails apply in the background
- One vendor, one contract, one operating model



Six reasons for AI Workspace by Myra

The best of both worlds



- One interface for all approved models
- Shared team projects keep knowledge in the organization
- Familiar frontier-model interface: intuitive from day one

Keep your data reliably secure



- Sensitive prompts stay on open-weight models in the EU
- No detour through US clouds
- Full control over every input
- Live security feedback helps users spot risks in every chat

Use AI that withstands every audit



- GDPR Art. 30 audit log: every request traceable
- Guardrails enforce your policies automatically
- Automated PII masking protects personal data

Avoid vendor lock-in



- Free choice among 20+ providers, including Mistral
- One endpoint keeps integrations simple
- Switch models without touching code

Keep your AI costs under control



- Budgets per organization, team, and user make spending predictable
- Every cost allocated to its source
- Exact-match cache: repeated requests are not billed twice
- Open-weight models on EU infrastructure lower token costs

Choose a sovereign security partner



- 100% EU shareholder structure
- No CLOUD Act exposure: your data stays under EU law
- Developed by a team delivering government-grade security since 2012

Everything a sovereign AI platform needs

Protection of personal data (PII masking)



- Detects names, email addresses, phone numbers, IBANs, and more
- Masks them before any data reaches the AI provider

Hosted on Myra's own sovereign EU infrastructure



- Open-weight models hosted in Germany for maximum data security
- No detour through US clouds

20+ provider integrations



- OpenAI, Anthropic, Google Gemini, Azure OpenAI, Mistral, and more
- The right model for every task, via one endpoint

Two-stage guardrail pipeline



- Fast in-process checks via regex and keywords
- Optional sidecars for NLP-PII, prompt guard, and tokenization
- Configurable per project, tenant, or user to match your policies

Budgets on three levels



- Spending limits per organization, department, and person
- Automatic resets and alerts prevent surprises on the invoice

Roles & permissions management



- Sensitive views only for authorized users
- Tiered from tenant admin to end user
- Every action documented in the audit log

Admin interface



- Tenants, gateways, users, and routing managed in one place
- Easy to operate via web interface
- Management views restricted to admins

Unified, OpenAI-compatible endpoint



- One endpoint for every model
- Automatic routing to the right provider
- Drop-in for existing SDKs: no code changes required

— TRANSPARENT PRICING MODEL

Built to fit. Easy to budget.

Step 1:

Define your number of seats

You decide what you need

From a single seat to an organization-wide plan.



Step 2:

Choose a platform according to your sovereignty needs

EU-located infrastructure

Hosting on infrastructure located in Europe.



EU-governed infrastructure

100% Myra-owned EU infrastructure with self-hosted open-weight models guarantees full EU data residency.



Step 3:

Define a model setup

20+ model providers available in AI Workspace



Rates depend on the models your teams choose, from Myra-hosted open-weight models to US frontier-tier models.

TOKEN COSTS BILLED BY MYRA

Bring your own key



Token usage is billed by your own provider under your existing contract.

NO TOKEN COSTS VIA MYRA

Mixed setup



Combine your own provider key(s) with the models available in AI Workspace. Pricing is individual.

INDIVIDUAL PRICING

— CERTIFICATIONS AND REFERENCES

Security proven for critical infrastructure since 2012

Certified, audited, operated in Germany

ISO 27001 BSI zertifiziert
auf der Basis von IT-Grundschutz
Zertifikat Nr.: BSI-IGZ-0667-2024



KRITIS
Nachweis gemäß
§ 8a, Abs. 3 BSIG



Selected references



Made in Germany



Unlock AI for your organization with powerful data protection and privacy guarantees.

Myra Security GmbH

+49 89 414141 - 345

www.myrasecurity.com

sales@myrasecurity.com

