

01 · STRATEGY

Creative power. Sovereign infrastructure.

A private, open-source-based AI content stack for global brands — built so your data, your models and your brand DNA never leave a sphere you control.

01

Data

Brand-critical inputs

Brand guidelines, product imagery, employee likenesses, strategy material and internal language. Anything fed into a vendor's pipeline is potentially compromisable the moment it leaves the controlled sphere.

02

Models

Brand DNA in weights

Specialised image and video models, brand-specific LoRAs and fine-tunes. With every production they embody more of your tone, characters and product context — over time, intellectual property that does not belong inside a foreign training pipeline.

100%

DATA CONTROL

Content, models and logs never leave your sphere.

0

VENDOR LOCK-IN

Heterogeneous stack, swappable per component.

∞

MODEL LIFETIME

Open-weights cannot be retracted by anyone.

02 · OUR APPROACH

Private-AI stack — six pillars.

Data sovereignty

Inputs and weights stay in the controlled...

Investment safety

Open-weight models cannot be...

Vendor independence

Heterogeneous stack — components...

Brand specialisation

LoRA and DreamBooth fine-tunes —...

Cost control at scale

Variable cost trends to electricity plus...

Compliance-ready

GDPR · EU AI Act · NIS2 · ISO 27001 ·...

03 · THE RISK SIDE

What today's SaaS AI doesn't solve.

01

Data leakage

Inputs and references can land in vendor training data — contractually, not technically excluded.

02

Model risk

Vendors introduce, change and retire models. API workflows can become obsolete without notice.

03

Lock-in

Workflows, prompt libraries and brand DNA inside a proprietary stack create super-linear switching cost.

04

Geopolitics & law

Blanket US/CN cloud contracts only partially satisfy GDPR, EU AI Act, NIS2 and sector regulation.

05

No real fine-tuning

Specialisation is mostly impossible, limited, or forces handing training material back to the vendor.

04 · ARCHITECTURE

Three zones, one pipeline.

Data sensitivity decides the location — not the contract.

01

ON-PREMISE

The core

Brand-critical IP. Customer-data fine-tuning. Production pipelines.

Stage-1 workloads · LoRAs · model repository

02

CONFIDENTIAL CLOUD

Burst capacity

Hardware-TEE, EU residency, no training reuse. Cryptographic attestation.

Stage-2 workloads · peak parallel · training

03

PUBLIC CLOUD

Cost-optimised

Where hourly price matters more than confidentiality.

Stage-3 · pre-vis · prototyping · spot capacity

05 · COMPLIANCE

Designed against the frameworks your auditors will name.

GDPR

EU AI ACT

NIS2

ISO 27001

TISAX

BAIT

NEXT STEP

Let's talk under NDA.

Request a confidential briefing on the private-AI stack, the hybrid architecture and the brand-specific fine-tuning

VAIN

office@vain.at

vain.at

Vienna · Austria