DORA.
EU AI Act.
CLOUD Act.

Three regulations. One problem.

Your entire operating environment

runs on infrastructure you don't control.

Enclave

We build sovereign platforms

for regulated European organisations.

One controlled operating environment.

Private AI

Inference and training on your sensitive data.

No external API’s

Private Developer platform

Source, CI/CD, registries.

Intellectual property never leaves the platform.

Deploy to dev, stage and production environments.

Private operations

Identity, collaboration, files, backups - governed.

Bring your own software.
Bring your own agents.
Bring your own models.

On a Sovereign platform your organisation then owns.

DORA-compliant from deployment.

Zero CLOUD Act exposure. Audit-ready.

Here's why you should trust this.

Early MVP.
We made a mistake.

Consumer NVME under enterprise workloads.

A cost decision that almost ended the company.

The cluster pushed the drives to 91°C.

K8s write patterns throttling the storage.

A year of building.
Hardware was about to die.


consumer NVMe at 91°C
THIS IS FINE.
running production etcd

Ordered enterprise drives. Emergency resilver.

All night. Offsite replication running in parallel.

Drive failure during the resilver...

...and everything would have been gone.

Everything held.

Barely.

Now every Enclave deployment

runs on full enterprise-grade components. By design.

So what does Enclave deliver today?

Sovereign Platform:

Sovereign Private AI capability

Local inference on sensitive data. EU AI Act compliant.

Sovereign Developer platform

Source control, CI/CD, registries. IP stays in the platform.

Sovereign Private operations

Identity, collaboration, storage, backup - governed access.

Turnkey delivery

Deployed, hardened, documented. Workshop training.

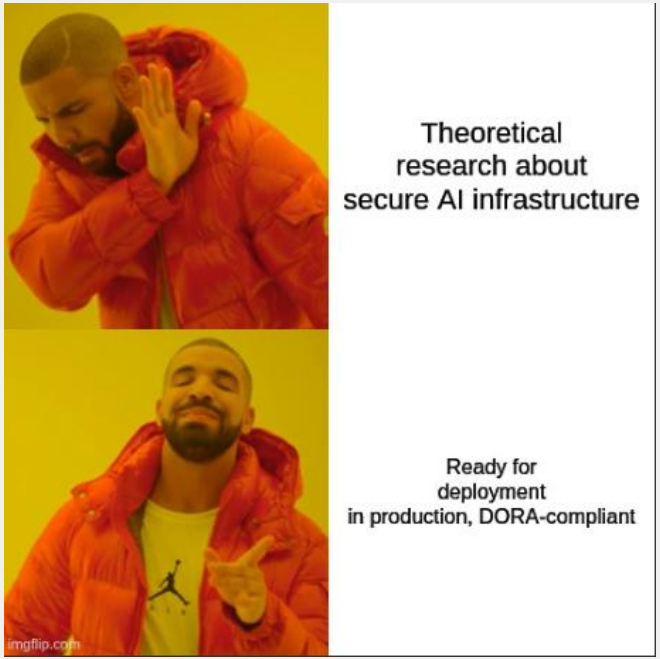
No vendor in the critical path.
No external dependency.
No exit strategy gap.

Most research consortia have

academic and industry researchers.

They don't have

a partner who's already got the production blueprint.


Theoretical
research about
secure AI infrastructure
Ready for
deployment
in production, DORA-compliant
imgflip.com

That's me.

The call I'm targeting:

SecureAI - *Enhancing the Security, Privacy and Robustness of AI Models and Systems*

Consortium partners wanted:

Industry partners

regulated sectors - fintech, legal, medtech, defence

SMEs

privacy-preserving and compliance

I'm the partner
your consortium should talk to.

Building Sovereign SecureAI?

Find me during the networking. For a full platform walkthrough and how we deploy our sovereign platforms.

Marcus

Founder · Enclave

0xenclave.com

Thanks.