



AI GOVERNANCE BRIEF

AUTHOR: HSG TECHNOLOGY TEAM

Where Does Your AI Run – and Who Controls Your Data?

Think of an AI model as an expert you hire to help your company.

CLOSED-SOURCE

Like hiring an outside consultant. You can use the company's expertise, but you cannot inspect or control what happens behind the scenes. Your employees may also be sending company information to the provider's servers.

OPEN-SOURCE

More like bringing that expert inside your building. Your company can download it, customize it and run it on systems you control.

But open-source does not automatically mean secure. An open-source model running on someone else's cloud is still outside your building. The most important question is:

Where does the AI run, and where does your data go?

A self-hosted model runs inside your company's digital walls. Proprietary information can remain on systems you control, protected by your own security rules. It is the difference between:

- Sending confidential documents to an outside consultant
- Bringing the consultant into a secure room where the documents never leave

Cloud-based AI can be appropriate for many business uses, especially with strong enterprise protections and contracts. But if your data cannot leave systems you control, self-hosting provides the clearest path.

Self-hosting still requires strong cybersecurity, access controls and monitoring. Owning the safe does not matter if you leave the door open.

The simplest way to remember it

OPEN OR CLOSED

Tells you who controls the model.

CLOUD OR SELF-HOSTED

Tells you who controls the environment.

YOUR SECURITY

Depends on understanding both.