



AI vendor due-diligence

The questions to ask before company data goes in.

Data

☐
☐
☐
☐

- Will you train on our data, and can we turn that off in writing?
- Where is our data stored, in which regions, and for how long?
- Who are your subprocessors, and how are we told when they change?
- On exit, how do we export our data, and how do you delete it?

Identity and access

☐
☐
☐

- Do you support single sign-on (SSO / SAML) and user provisioning?
- Are there admin roles and per-user access controls?
- Can an admin see usage and pull audit logs?

Security and assurance

☐
☐
☐

- Do you have SOC 2 Type II or ISO 27001, and can we see the report?
- Do you run penetration tests, and will you share a summary?
- What is your breach history and notification commitment?

Output and safety

☐
☐

- Can we keep a human in the loop for consequential actions?
- What protects against prompt injection and data leakage?

Get training-off and company sign-on right first; those two prevent the worst outcomes. Tighten the rest as you go.

AEGYS · aegys.io · secure@aegys.io