nine

AI Compliance Checklist

What questions do you need to ask before building AI infrastructure?

You're running documents through an AI model, analysing customer data or training your own models – this is sensitive information, trade secrets and proprietary content. Companies running this data on US hyperscalers risk unwanted access by US authorities (CLOUD Act), compliance violations and liability. This checklist helps you ask the right questions.

1 Data Sovereignty & Jurisdiction

- [ ] Where is my training and inference data physically stored?
- [ ] Can US authorities demand access to my data without notifying me?
- [ ] Is my provider subject to US jurisdiction, even if their servers are located in Europe?
- [ ] Is jurisdiction contractually governed by Swiss law?
- [ ] Have I signed a Data Processing Agreement (DPA)?

2 Regulatory Requirements & Oversight

- [ ] What regulatory requirements apply to my industry for data storage and outsourcing (FINMA 2008/7, HMG, cantonal DSG)?
- [ ] Are AI outsourcing arrangements covered in my outsourcing policy?
- [ ] Have I documented exit strategies and contingency plans?
- [ ] Can audit and supervisory authorities access systems and logs if required?
- [ ] Are responsibilities for AI-driven decisions clearly defined?

3 Data Protection (nDSG / GDPR)

- [ ] What personal data flows into my AI models?
- [ ] Have I carried out a Data Protection Impact Assessment (DPIA)?
- [ ] Is training and inference data pseudonymised or anonymised?
- [ ] How long is data retained and who has access?
- [ ] Are data subject rights (access, erasure) guaranteed?

4 Security & Certifications

- [ ] Is my infrastructure provider ISO 27001 certified?
- [ ] Are regular security audits and penetration tests conducted?
- [ ] Are backup and disaster recovery processes defined and tested?
- [ ] What SLAs apply for availability and response times?
- [ ] Are access rights and network isolation clearly defined?

5 Technical Requirements

- [ ] What GPU specifications do I need (training vs. inference)?
- [ ] Do I need dedicated hardware or is shared infrastructure sufficient?
- [ ] How do I scale as requirements grow?
- [ ] Do I have a direct technical contact person?
- [ ] Is network latency and bandwidth sufficient for my workloads?

6 Provider Selection & Contracts

- [ ] Where is my provider headquartered and where are their data centres?
- [ ] Does my provider itself use US sub-processors, and if so, for which services?
- [ ] What certifications does the provider hold (ISO 27001, ISO 9001)?
- [ ] Is there a personal contact instead of anonymous support?
- [ ] How is the provider reachable in a crisis (24/7)?