

Data Protection & Governance in AI Projects

AI projects are a leadership responsibility — not just an IT topic.

- AI processes customer, employee, contract and operational data.
- Data protection, security and the business unit decide together.
- Without governance: shadow AI, data leakage, liability risks.

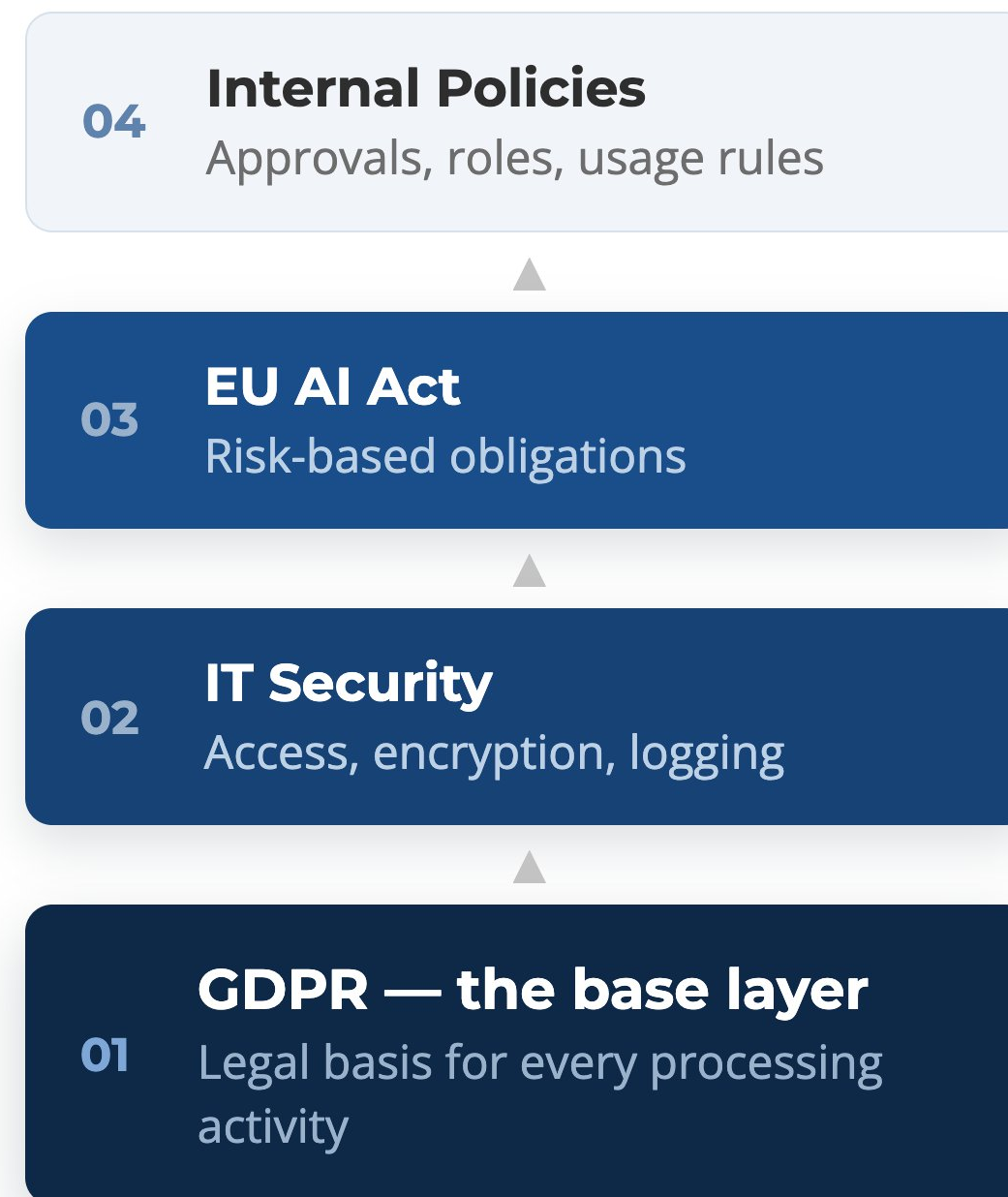


The GDPR remains the foundation

The EU AI Act does not replace data protection — it is added on top of it.

- Purpose limitation, data minimisation, a legal basis and transparency still apply.
- AI models trained on personal data are not automatically anonymous.
- Particularly sensitive: customer, employee, health and applicant data.

Source: EDPB Opinion 28/2024; EU AI Act.



The AI Act changes how projects are assessed

Companies must assess, on a risk basis, which AI they deploy.

- Prohibited AI practices have applied since February 2025.
- Obligations for general-purpose and high-risk AI take effect in stages.
- SMEs are rarely providers — usually the “deployer” of AI systems.

Source: European Commission, AI Act Framework.

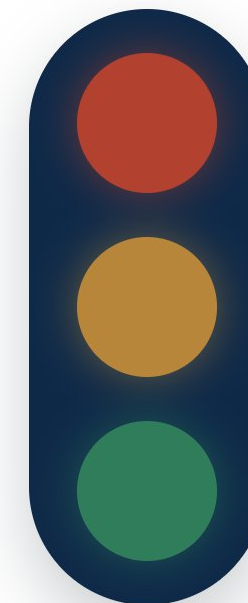


Which data may go into AI?

Not every piece of information belongs in prompts, training data or knowledge bases.

- Before use: define clear data classes.
- Handle contracts, personnel files and trade secrets separately.
- Default rule: as little personal data as possible.

Source: BfDI & DSK — data protection review before AI use.



Red — Personal & confidential

Only with a legal basis and review

Amber — Internal business data

Only in approved, secure systems

Green — Public content

Largely uncritical to use

Shadow AI is the biggest practical risk

Without a secure solution, employees often use unvetted tools.

- Typical: chatbots for customer texts, applications, contracts, meeting notes.
- Risk: confidential content leaves the company uncontrolled.
- Solution: define permitted tools, prohibited data and approval paths.

SECURE AI USE — FRAMEWORK

- ✓ **Permitted tools**
Approved, vetted applications
- ✓ **Permitted data types**
Clear limits per the data traffic light
- ✓ **Approval process**
Who approves new use cases?
- ✓ **Logging**
Traceability of use
- ✓ **Training**
Enable employees to use AI safely

Who may do what with which AI?

AI needs roles, permissions and traceable decisions.

Role	Responsibility	Strategy	Selection	Operation	Control
Executive Leadership	Guardrails & risk appetite	A	A	I	I
Business Unit	Purpose, benefit & factual accuracy	C	R	A	R
IT	Security & data processing	C	R	R	C
Data Protection	Admissibility, contracts & rights	C	C	C	A
Procurement	Sourcing & vendor management	I	R	I	I

Vendor due diligence is mandatory, not a formality

The vendor co-determines data protection, availability and liability.

- Check: server location, data processing agreement, sub-processors, use for training.
- Check: logging, deletion concept, export capability, permissions.
- For sensitive data: EU hosting, private instances or local AI.

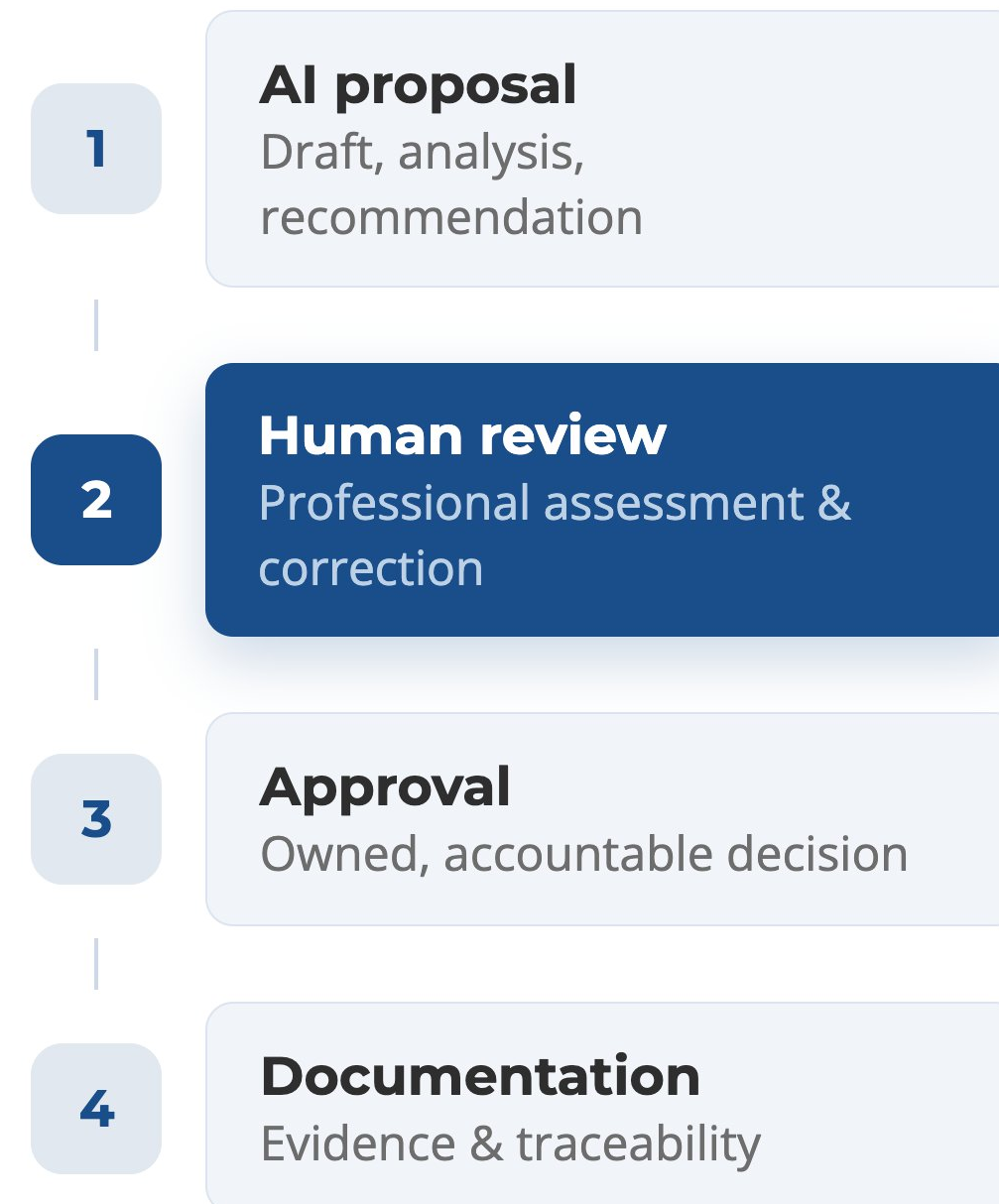
VENDOR SCORECARD	Rating 1-5
Data protection Location, DPA, use for training	○ ○ ○ ○ ○
Security Logging, encryption, permissions	○ ○ ○ ○ ○
Contract DPA, liability, SLA	○ ○ ○ ○ ○
Operation Availability, support, deletion	○ ○ ○ ○ ○
Exit Export, migration, data return	○ ○ ○ ○ ○

Human oversight remains decisive

AI may prepare decisions — but must not make critical decisions unchecked.

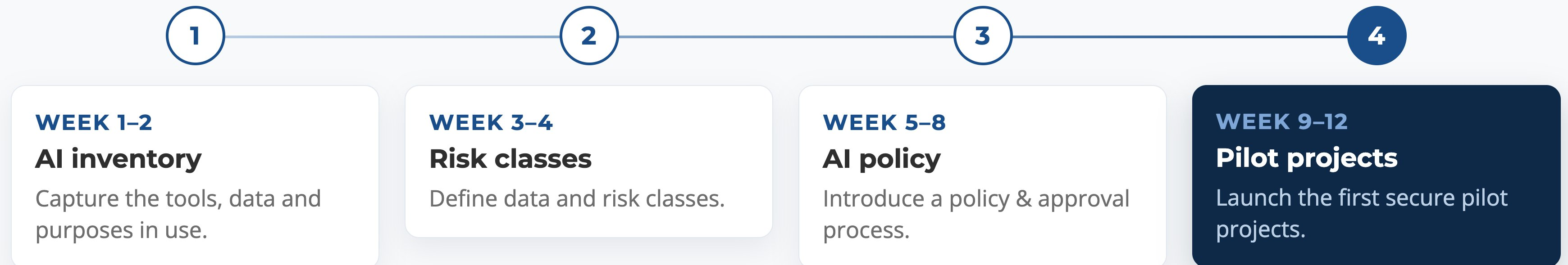
- Relevant in HR, customer scoring, credit, compliance, medicine, safety.
- Anchor professional control firmly within the process.
- Results stay reviewable, correctable and documentable.

Source: AI Act — human oversight, monitoring, logging for high-risk AI.



Recommended 90-day roadmap

Good AI governance can be started pragmatically.



Data protection & governance don't slow AI down — they make AI usable.

PATH A — STATUS QUO

Allow uncontrolled tool use

Shadow AI, uncontrolled data leakage and liability risks.

vs

PATH B — RECOMMENDATION

Build controlled AI capability

Immediate measure: AI policy, tool approval and the data traffic light — productive use at reduced risk.

NEXT STEP

Run the KrambergAI AI governance check and prioritise measures.



KrambergAI
krambergai.com