

## **Describing functionality of your AI Model**

Funding programmes seek clarity, structure, and well-thought-out strategies.

The three key questions are:

**Does the team understand the technology?**

**Is the data strategy viable?**

**Have ethics, security, and regulations been considered?**

### **1. Technical Feasibility – Demonstrating Your Technical Expertise**

#### **1.1 AI Approach & Functionality**

- What type of AI are you using? (e.g., Machine Learning, Deep Learning, NLP, Computer Vision)
- What algorithms or models are applied? (e.g., Transformer models, CNNs, Decision Trees)
- How is the AI trained and updated? (e.g., supervised, unsupervised, transfer learning)
- What architecture are you using? (Cloud-based, On-Premise, Edge AI?)

#### **1.2 Team's Technical Expertise**

- Who are the key team members, and what AI expertise do they bring?
- Are there relevant publications, patents, or previous projects?
- If expertise is missing: Do you have external advisors, mentors, or partnerships?

### **2. Data Strategy – Showing That You Have Thought Through Data Sources and Quality**

#### **2.1 Data Sources & Availability**

- What data do you use? (structured/unstructured, public/private, own/external)
- How is the data collected? (APIs, web scraping, partnerships)
- Is there sufficient data for training and validation?
- If data is limited: What strategies do you use? (synthetic data, transfer learning, federated learning)

#### **2.2 Data Quality & Bias Management**

- How do you ensure that your data is of high quality?
- What measures do you take against biases?
- Do you have a strategy for continuous data validation?

### **3. Ethics, Data Security & Regulations – Demonstrating Responsible AI Practices**

#### **3.1 Ethical Considerations**

- What risks does your AI pose? (e.g., discrimination, manipulation, misinformation)
- How do you minimize negative societal impacts? (e.g., transparency, fairness checks, audits)

#### **3.2 Data Security & Privacy**

- How do you protect personal or sensitive data? (e.g., encryption, anonymization, GDPR compliance)
- What security measures are in place against misuse or cyberattacks?

#### **3.3 Regulatory Requirements (AI Act & More)**

- Into which risk category of the **EU AI Act** does your AI fall?
- What measures are you implementing to comply with regulatory requirements?
- Do you already have certifications or evaluation mechanisms for your AI?