ÖPAG Fraud Detection Requirements:

Use Case & Requirements

- Detection of falsified or manipulated documents, including deepfake and AI-generated content.
- Document-based fraud detection: Analysis of documents for irregularities or anomalies, e.g., structural breaks, metadata inconsistencies, or layout anomalies.
- Detection of visual and content-related forgery indicators (e.g., font deviations, retouched areas, inconsistent data).
- API interfaces for integration into our existing platform.
- Process support: No straight-through processing. The fraud detection solution must support the process but must not make the final decision within the workflow.

Technical & Data Protection Requirements

- The operating model must support on-premises, cloud, or hybrid solutions.
- The solution must be GDPR-compliant.
- Processing exclusively in data centers located within Europe. Data processing must take place within the EU.
- No data transfer to third countries (especially the USA), not even via subcontractors or distributed cloud infrastructures.
- Clear statements on data security, encryption, and data deletion.

Contribution of a Challenge Participant

We kindly ask you to provide the following information:

1. Brief company introduction and relevance of your solution for the use case described above.
2. Functional description of your fraud detection technology (including current use cases or references in the banking or financial sector).
3. Technical architecture (API, integration, operating model, reporting).
4. Information on data protection, data processing, and hosting location.
5. Options for conducting a Proof of Concept (PoC), including timeframe and technical scope.
6. Indication of licensing models and pricing structure.