

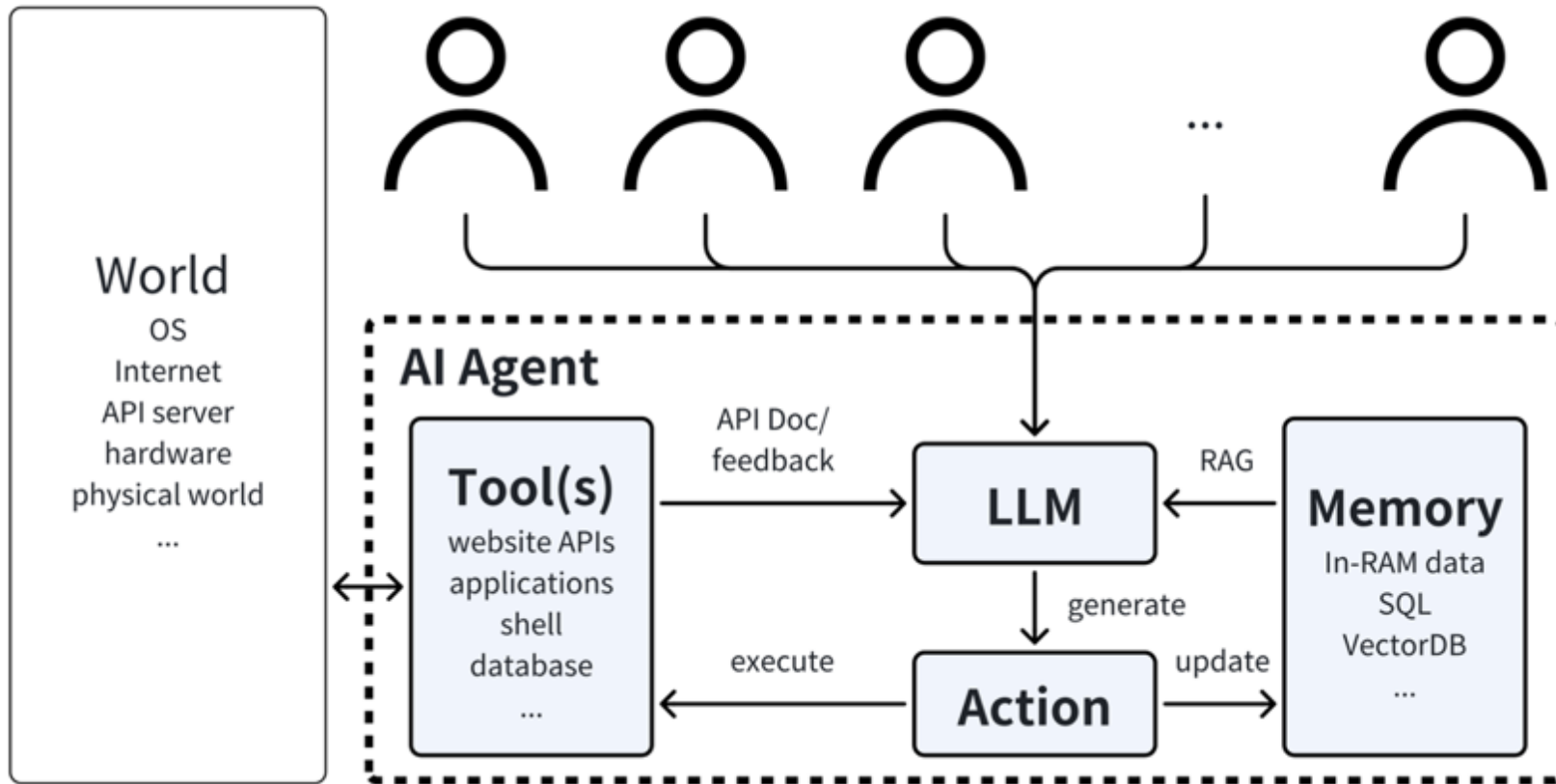


**UNIVERSITY OF APPLIED
SCIENCES AND ARTS**

Privacy-Preserving Federated Data Spaces for Agentic LLM Processes

Dr. Ing. Koen Gilissen
Successful R & I in Europe 2026

Agents



HORIZON-CL3-2027-01-FCT-01: Online harms detection and investigation tools using a short development cycle model

Developing a secure, autonomous AI, investigative assistant for Law Enforcement
Orchestration of multiple LLM agents to scan, categorize, and link online harms
(disinformation, illegal content)

Core Scope

Innovation Action (IA)

- Online Harms Detection
- Safeguarding online spaces
- Investigation Tools
- Detection Tools

- Short Development Cycle
- Rapid prototyping
- Agile deployment

Added Value

- Security-by-Design
- Privacy-by-Design
- Agentic Safe Operate
- Formal Verification
- Least Privilege Protocols
- Adversarial Resilience
- Vulnerability mitigations
- Operational Validation
- Real-world pilot
- Cross-border validation

scientific and technological expertise



MAI-HOME

MLSecOps

- Energy
- Predictive maintenance
- Citizen Data Privacy Protection
- Security awareness
- Secure ML development



REAL

Data security

- CSRD
- Human Centric Data
- Sustainability
- Industry 5.0
- Resillience



TETRA VCSOP: LLASER

Privacy & Security of LLMs Integrations

- Threat models
- Privacy threats
- Security threats
- Mitigations

We are looking for...



Law Enforcement Agencies (LEAs)



Forensic Specialists



AI Ethics & Fundamental Rights Experts



Social Sciences and Humanities (SSH) Experts



Business Innovation & Market Uptake Specialists

Thank you for listening



Dr. Ing. Koen Gilissen



koen.gilissen@pxl.be



<http://www.linkedin.com/in/koengilissen>