

AI agents fail on data access: How Swiss SMEs become agent-ready

MANAGEMENT SUMMARY & CORE TAKEAWAY

AI agents rarely fail because of the model; they fail because they cannot access the right data. MCP reduces integration effort from $O(N \times M)$ to $O(N+M)$. Swiss SMEs need three layers: MCP servers per system, a federated query layer, and identity-based permissions—otherwise agents remain chatbots.

CONTEXT & EXECUTIVE RELEVANCE

Most SME AI-agent projects fail not because the model is weak, but because the agent cannot access the right data at the right time. Swiss SMEs typically run 3 to 8 core systems—ERP, CRM, DMS, HR, ticketing—each with its own API, permissions, and data format. The result is agent sprawl: many half-finished agents that see only a slice of the truth.

The Model Context Protocol (MCP) has emerged as the de facto standard. It connects AI agents to tools and data sources through a uniform protocol—described by SAS as a "USB-C port for AI." In December 2025, MCP was transferred to the Agentic AI Foundation under the Linux Foundation. The protocol now sees 97 million monthly SDK downloads.

CORE ACTION ITEMS

01 Agents only access one system and give incomplete answers

02 Permissions are configured manually per tool and drift apart

03 Every new integration costs $O(N \times M)$ effort instead of $O(N+M)$

SWISS COMPLIANCE & ARCHITECTURE GUIDELINES

- ☑ Full compliance with revised Swiss Data Protection Act (revDSG).
- ☑ Zero vendor lock-in on closed proprietary models.
- ☑ Seamless integration into Abacus, Bexio and M365 ecosystems.

Non-Binding Process Analysis

Let us review in 20 minutes where AI agents create immediate measurable efficiency in your workflows.

ki-outsourcing.ch