

# Shadow Agents: The New Compliance Challenge for SMEs

## MANAGEMENT SUMMARY & CORE TAKEAWAY

Shadow agents are AI systems that act on their own: they send emails, book appointments, or trigger payments. Unlike shadow AI, they carry independent legal responsibility. Without governance, you risk data breaches, uncontrolled actions, and liability. The first step is clear rules and human final decision-making.

## CONTEXT & EXECUTIVE RELEVANCE

Shadow AI was primarily a confidentiality problem: employees manually entered data into chatbots. Shadow agents go further—they act autonomously. They draft and send emails, book meetings, trigger payments. This shift from passive tool to active system fundamentally changes the risk profile. Once agents gain access to systems and data, a new quality of responsibility emerges.

Classic controls mostly track which devices and services are used. They do not detect what an agent actually does. New attack vectors emerge here: prompt injection, where manipulated inputs trick an agent into unwanted actions, or manipulation of entire agent networks. Without AI policies, these risks go unmanaged.

## CORE ACTION ITEMS

- 01 Create an inventory: Which AI agents or automations are active in your company?
- 02 Define minimal governance rules: Who may do what? Where is human approval mandatory?
- 03 Introduce access rights and logging: Every agent action must be traceable.
- 04 Assign responsible persons: For each system, one person who is accountable.

## SWISS COMPLIANCE &amp; 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](https://ki-outsourcing.ch)