novaeon

DIE CHECKLISTE · 40 PRÜFPUNKTE

KI-Agenten in Produktion bringen

Novaeon Studio · Maik Buchenau · Stand November 2026

Ein KI-Agent handelt in Finanzwesen, Personalwesen, Einkauf oder Vertrieb – mit echten Berechtigungen und echten Folgen. Diese Checkliste behandelt jeden Agenten wie jede andere Änderung in SAP: inventarisiert, bewertet, getestet, freigegeben, überwacht und rücknehmbar, wie ein Transport. Sie gilt für SAP-Joule-Agenten (durchgängig als Beispiel verwendet), eigene Agenten auf SAP BTP und Agenten anderer Anbieter, die auf Ihre SAP-Daten zugreifen. 40 Prüfpunkte in 9 Blöcken. Haken Sie sie ab, markieren Sie die Lücken und benennen Sie für jeden Punkt einen Verantwortlichen.

> Hinweis: SAP entwickelt Joule und Joule Studio sehr schnell weiter. Prüfen Sie Termine, Preise und Verfügbarkeit (GA/EA/Roadmap) vor jeder Entscheidung anhand der aktuellen SAP-Dokumentation und Ihres eigenen Vertrags. Allgemeine Information, keine Rechtsberatung. Mit KI erstellt.

1 Inventar & Verantwortung

- [ ] Jeder Agent hat einen **fachlichen Verantwortlichen** (Prozessverantwortung) und einen technischen Verantwortlichen (Betrieb).
- [ ] Jeder Agent steht in **einem Inventar**, einschließlich der Modelle, Skills, Sub-Agenten und MCP-Server, die er nutzt. In SAP-Landschaften ist das der **SAP AI Agent Hub** (aus LeanIX), der auch Agenten anderer Anbieter aufführt.
- [ ] Zweck, Prozess, betroffene Systeme und Datenkategorien sind in einem Satz dokumentiert („Was darf dieser Agent tun, und was nicht?“).
- [ ] Agenten außerhalb von SAP, die auf SAP-Daten zugreifen (Copilot, eigene Agenten über A2A/MCP), stehen im selben Inventar.

2 Risiko & Autonomie

- [ ] Jeder Agent hat eine Risikoeinstufung (z. B. niedrig / mittel / hoch) nach Auswirkung: Geld, Menschen, Kunden, Compliance.
- [ ] Der **Autonomiegrad** ist eine bewusste Entscheidung: nur vorschlagen · mit Freigabe handeln · eigenständig handeln.
- [ ] **Human-in-the-loop** ist für jeden Schritt mit hohem Risiko eingerichtet (ein Mensch gibt frei, nicht nur ein Protokolleintrag).
- [ ] Geprüft, ob der Anwendungsfall unter **Anhang III des EU AI Act** fällt (z. B. Einstellung, Beförderung, Leistungsbeurteilung). Die Pflichten für Hochrisiko-Systeme gelten ab dem 2. Dezember 2027.

3 Identität & Berechtigungen

- [ ] Der Agent handelt nur mit den Berechtigungen des anfragenden Benutzers (Schnittmenge aus Benutzer und Agent); autonome Agenten haben eine **eigene technische Identität**.
- [ ] Rollen und Berechtigungen des Agenten sind im Berechtigungskonzept beschrieben und freigegeben. Kein „SAP_ALL für den Bot".
- [ ] Ausgehende Verbindungen (Destinations, OAuth) folgen dem Muster Client Credentials (Maschine-zu-Maschine) oder JWT bearer (User Propagation); keine Secrets im Code.
- [ ] Eigene Agenten auf BTP Cloud Foundry sind mit IAS abgesichert. Andernfalls sind sie standardmäßig aus dem Internet erreichbar.
- [ ] In Produktion werden nur **verifizierte MCP-Server** aufgerufen.

4 Daten & Grounding

- [ ] Hochgeladene Grounding-Dokumente geprüft: In Joule sind sie für **alle Benutzer des Tenants** sichtbar (keine Berechtigungen pro Dokument). Laden Sie nichts Vertrauliches hoch.
- [ ] Stammdatenqualität für den Prozess bewertet (ein Agent, der mit schlechten Daten arbeitet, trifft falsche Entscheidungen nur schneller).
- [ ] Entscheidung über die Nutzung von Kundendaten durch den Anbieter getroffen (bei SAP: Opt-out in SAP for Me); Logging-Opt-in bewusst gesetzt.
- [ ] Datenschutz: Verzeichnis von Verarbeitungstätigkeiten, DSFA wo erforderlich, und Rechenzentrumsregion (z. B. EU Access) dokumentiert.

5 Test & Evaluierung

- [ ] Testfälle existieren für die Hauptabläufe **und** für Grenzfälle (fehlende Daten, widersprüchliche Anweisungen, abgebrochene Läufe).
- [ ] Sicherheitstests: Prompt Injection, Tool-Missbrauch, Datenabfluss über Antworten.
- [ ] Evaluierungsszenarien mit erwarteten Ergebnissen; Abnahmekriterien vorab vereinbart (z. B. Trefferquote, Fehlertoleranz).
- [ ] Tests prüfen nicht nur, dass Tools **gefunden**, sondern dass sie tatsächlich **aufgerufen** werden (Discovery ≠ Invocation): Ein Tool, das in der Liste erscheint, beweist nicht, dass der Agent es aufrufen kann – testen Sie daher echte Aufrufe Ende-zu-Ende.
- [ ] Regressionstest nach jedem SAP-Release-Update und jeder Änderung am Agenten eingeplant.

6 Transport & Freigabe

- [ ] Getrennte Umgebungen Entwicklung → Test → Produktion; keine Entwicklung direkt in Produktion.
- [ ] Transportweg definiert: Joule Studio classic über **Cloud Transport Management** (MTA); neues Joule Studio über Git-basierte Deployments; eigene Agenten über Ihre eigene CI/CD-Pipeline.
- [ ] Jede Änderung (Prompt, Anweisungen, Tools, Modellwechsel) wird **versioniert** und durchläuft dieselbe Freigabe wie Code.
- [ ] Formale Freigabe vor dem Go-live (Change Request, Freigebender, Datum), z. B. in **SAP Cloud ALM**.
- [ ] Release-Abhängigkeiten geklärt: Joule-Funktionen kommen nur mit aktuellen Releases. Ihr Upgrade-Kalender ist Ihr KI-Kalender.

7 Betrieb & Monitoring

- [ ] Laufendes Monitoring: Nutzung, Fehlerquote, Antwortzeiten, Abbrüche (Agent Hub / Cloud ALM, soweit verfügbar).
- [ ] Nachvollziehbarkeit: Audit Trail je Session, der zeigt, wer was mit welchem Ergebnis ausgelöst hat.
- [ ] Verhaltensdrift beobachtet (z. B. Process/Agent Mining in Signavio, Stichproben durch den Verantwortlichen).
- [ ] Incident-Prozess: Eine benannte Person wird alarmiert, wenn ein Agent falsch handelt, und eine benannte Person (meist der fachliche Verantwortliche) darf ihn abschalten.

8 Kosten

- [ ] Verbrauch je Agent geschätzt: SAP-Agenten **0,02 AI Units pro Agent-Aktion** (2026); eigene Agenten nach Ressourcenverbrauch.
- [ ] Ende der kostenfreien Laufzeit für eigene Joule-Agenten (**31. Dezember 2026**) im Budget 2027 berücksichtigt.
- [ ] Budget **pro Agent**, nicht pro Benutzer; Warnschwelle und harte Obergrenze definiert (AI Units verfallen nach 12 Monaten).
- [ ] Vertragskonditionen verhandelt: Preis pro AI Unit, Kontingent, Preis für Mehrverbrauch und ob nicht genutzte Units übertragen werden können (standardmäßig verfallen sie nach 12 Monaten).
- [ ] Deterministische Schritte als **Skills** statt als Agent-Schritte umgesetzt (Joule Skills werden nicht pro Aufruf abgerechnet).

9 Betriebsrat, Rollback & Stilllegung

- [ ] **Betriebsrat** frühzeitig eingebunden, wo Mitbestimmung greift. In Deutschland: § 90 BetrVG (erfasst KI ausdrücklich) und § 87 Abs. 1 Nr. 6 BetrVG (Systeme, die Verhalten oder Leistung überwachen können). In der Regel ist dafür eine Betriebsvereinbarung nötig.
- [ ] Rollback-Plan getestet: vorherige Version wiederherstellen oder den Agenten abschalten, ohne den Prozess anzuhalten (manueller Fallback).
- [ ] Kriterien für die Stilllegung definiert (Nutzen, Kosten, Fehlerquote) und je Agent ein regelmäßiger Überprüfungstermin festgelegt.
- [ ] Die Stilllegung räumt auf: Berechtigungen, Destinations, Inventareintrag, Grounding-Dokumente.

Novaeon Studio — SAP-Release- und Change-Management trifft KI-Agenten.
Sie möchten Ihre Agenten anhand dieser Liste durchgehen? Vereinbaren Sie ein 30-minütiges Gespräch: https://novaeon.studio/de/contact/ · office@novaeon.studio