novaeon

CHECKLIST-UL · 40 DE PUNCTE DE CONTROL

# Agenți AI în producție

Novaeon Studio · Maik Buchenau · Versiunea noiembrie 2026

Un agent AI acționează în finanțe, HR, achiziții sau vânzări, cu autorizații reale și consecințe reale. Acest checklist tratează fiecare agent ca pe orice altă modificare în SAP: inventariat, evaluat, testat, aprobat, monitorizat și reversibil, la fel ca un transport. Se aplică agenților SAP Joule (folosiți ca exemplu pe tot parcursul documentului), agenților proprii pe SAP BTP și agenților altor furnizori care accesează datele dumneavoastră SAP. 40 de puncte de control în 9 blocuri. Bifați-le, marcați lacunele și numiți un responsabil pentru fiecare.

> Notă: SAP dezvoltă Joule și Joule Studio foarte rapid. Înainte de orice decizie, verificați datele, prețurile și disponibilitatea (GA/EA/roadmap) în documentația SAP actuală și în propriul dumneavoastră contract. Informații generale, nu consultanță juridică. Redactat cu ajutorul AI.

## 1 Inventar & responsabilitate

- [ ] Fiecare agent are un **responsabil de business** (răspunderea pentru proces) și un responsabil tehnic (operare).
- [ ] Fiecare agent figurează într-un **singur inventar**, inclusiv modelele, skill-urile, sub-agenții și serverele MCP pe care le folosește. Pentru landscape-urile SAP, acesta este **SAP AI Agent Hub** (din LeanIX), care listează și agenți ai altor furnizori.
- [ ] Scopul, procesul, sistemele afectate și categoriile de date sunt documentate într-o singură frază („Ce are voie acest agent să facă și ce nu?”).
- [ ] Agenții din afara SAP care accesează date SAP (Copilot, agenți proprii prin A2A/MCP) figurează în același inventar.

## 2 Risc & autonomie

- [ ] Fiecare agent are o evaluare a riscului (de ex. scăzut / mediu / ridicat) în funcție de impact: bani, oameni, clienți, conformitate.
- [ ] **Nivelul de autonomie** este o decizie asumată: doar propune · acționează cu aprobare · acționează autonom.
- [ ] **Human-in-the-loop** este configurat pentru fiecare pas cu risc ridicat (o persoană aprobă, nu doar o înregistrare în log).
- [ ] S-a verificat dacă scenariul de utilizare intră sub incidența **Anexei III din EU AI Act** (de ex. recrutare, promovare, evaluarea performanței). Obligațiile pentru sistemele cu risc ridicat se aplică începând cu 2 decembrie 2027.

## 3 Identitate & autorizații

- [ ] Agentul acționează doar cu permisiunile utilizatorului care face solicitarea (intersecția dintre utilizator și agent); agenții autonomi au o **identitate tehnică proprie**.
- [ ] Rolurile și autorizațiile agentului sunt descrise în conceptul de autorizații și aprobate. Fără „SAP_ALL pentru bot".
- [ ] Conexiunile de ieșire (destinations, OAuth) urmează modelul client credentials (machine-to-machine) sau JWT bearer (propagarea utilizatorului); fără secrete în cod.
- [ ] Agenții proprii care rulează pe BTP Cloud Foundry sunt securizați cu IAS. Altfel, sunt accesibili din internet în mod implicit.
- [ ] În producție sunt apelate doar **servere MCP verificate**.

## 4 Date & grounding

- [ ] Documentele de grounding încărcate au fost verificate: în Joule sunt vizibile pentru **toți utilizatorii tenantului** (fără permisiuni la nivel de document). Nu încărcați nimic confidențial.
- [ ] Calitatea datelor master pentru proces a fost evaluată (un agent care lucrează pe date proaste doar ia decizii greșite mai repede).
- [ ] S-a luat o decizie privind utilizarea datelor clienților de către furnizor (pentru SAP: opt-out în SAP for Me); opt-in-ul pentru logging este setat în mod deliberat.
- [ ] Protecția datelor: registrul activităților de prelucrare, DPIA acolo unde este necesar și regiunea centrului de date (de ex. EU Access) sunt documentate.

## 5 Testare & evaluare

- [ ] Există cazuri de test pentru fluxurile principale **și** pentru cazurile-limită (date lipsă, instrucțiuni contradictorii, rulări întrerupte).
- [ ] Teste de securitate: prompt injection, utilizarea abuzivă a tool-urilor, scurgeri de date prin răspunsuri.
- [ ] Scenarii de evaluare cu rezultate așteptate; criterii de acceptanță convenite de la început (de ex. rata de reușită, toleranța la erori).
- [ ] Testele verifică nu doar că tool-urile sunt **descoperite**, ci și că sunt efectiv **apelate** (descoperire ≠ apelare): un tool care apare în listă nu dovedește că agentul îl poate apela, așa că testați apeluri reale end-to-end.
- [ ] Test de regresie planificat după fiecare actualizare de release SAP și după fiecare modificare a agentului.

## 6 Transport & aprobare

- [ ] Medii separate de dezvoltare → test → producție; nu se construiește direct în producție.
- [ ] Calea de transport este definită: Joule Studio clasic prin **Cloud Transport Management** (MTA); noul Joule Studio prin deployment-uri bazate pe Git; agenții proprii prin propriul pipeline CI/CD.
- [ ] Fiecare modificare (prompt, instrucțiuni, tool-uri, schimbarea modelului) este **versionată** și trece prin aceeași aprobare ca și codul.
- [ ] Aprobare formală înainte de go-live (change request, aprobator, dată), de ex. în **SAP Cloud ALM**.
- [ ] Dependențele de release sunt clarificate: funcționalitățile Joule vin doar cu release-urile actuale. Calendarul dumneavoastră de upgrade este calendarul dumneavoastră AI.

## 7 Operare & monitorizare

- [ ] Monitorizare continuă: utilizare, rata de erori, timpi de răspuns, întreruperi (Agent Hub / Cloud ALM, acolo unde sunt disponibile).
- [ ] Trasabilitate: audit trail per sesiune, care arată cine a declanșat ce și cu ce rezultat.
- [ ] Derivele de comportament sunt urmărite (de ex. process/agent mining în Signavio, verificări prin sondaj de către responsabil).
- [ ] Proces de incident: o persoană desemnată este alertată când un agent acționează greșit, iar o persoană desemnată (de regulă responsabilul de business) are dreptul să îl oprească.

## 8 Costuri

- [ ] Consumul este estimat per agent: agenți SAP **0,02 AI Units per acțiune a agentului** (2026); agenți proprii în funcție de consumul de resurse.
- [ ] Sfârșitul runtime-ului gratuit pentru agenții Joule proprii (**31 decembrie 2026**) este inclus în bugetul pe 2027.
- [ ] Buget **per agent**, nu per utilizator; prag de avertizare și limită strictă definite (AI Units expiră după 12 luni).
- [ ] Condițiile contractuale sunt negociate: prețul per AI Unit, volumul inclus, tariful pentru depășire și dacă unitățile neutilizate pot fi reportate (implicit, acestea expiră după 12 luni).
- [ ] Pașii deterministi sunt construiți ca **skill-uri**, nu ca pași de agent (skill-urile Joule nu sunt taxate per apel).

## 9 Consiliul angajaților, rollback & scoatere din uz

- [ ] **Consiliul angajaților** (Betriebsrat) este implicat din timp acolo unde se aplică dreptul de codecizie. În Germania: § 90 BetrVG (acoperă explicit AI) și § 87(1) no. 6 BetrVG (sisteme capabile să monitorizeze comportamentul sau performanța). De regulă, este necesar un acord de întreprindere (Betriebsvereinbarung).
- [ ] Planul de rollback este testat: restaurarea versiunii anterioare sau oprirea agentului fără oprirea procesului (fallback manual).
- [ ] Criteriile de scoatere din uz sunt definite (valoare, cost, rata de erori) și pentru fiecare agent este stabilită o dată de revizuire periodică.
- [ ] Scoaterea din uz include curățenia: autorizații, destinations, intrarea din inventar, documentele de grounding.

**Novaeon Studio** — release și change management SAP, aplicate agenților AI.
Doriți să vă analizăm agenții pe baza acestei liste? Programați o discuție de 30 de minute:
https://novaeon.studio/ro/contact/ · office@novaeon.studio