

INTERNÍ SCHVÁLENÍ AGENTA

Co musí být hotové, než agent přejde do pilotu nebo produkce.

Dokumentace připravena

Jednostránková specifikace agenta vyplněná a podepsaná. ☐ ANO ☐ NE

Akceptační kritéria a 2–4 metriky úspěšnosti. ☐ ANO ☐ NE

Pět testovacích scénářů s výsledky (vč. halucinace a citlivých dat). ☐ ANO ☐ NE

Analýza rizik a mitigací (halucinace, bias, citlivá data). ☐ ANO ☐ NE

Auditní plán: logy, verze, dohledatelnost vstupů a výstupů. ☐ ANO ☐ NE

Role přidělené

Vlastník procesu – drží metriky a rozhoduje o změnách. ☐ ANO ☐ NE

Klíčová role. Bez ní nepokračovat.

Technický garant (IT) – přístupy, integrace, provoz. ☐ ANO ☐ NE

Právní garant – posouzení GDPR a interních pravidel. ☐ ANO ☐ NE

Operátoři / uživatelé – proškoleni a vědí, jak hlásit chybu. ☐ ANO ☐ NE

Schvalovací kroky proběhly

1. Návrh agenta (role, vstupy/výstupy, metriky). ☐ ANO ☐ NE

2. Technická kontrola (integrace, přístupy, logování). ☐ ANO ☐ NE

3. Právní a bezpečnostní posouzení. ☐ ANO ☐ NE

4. Pilotní nasazení odsouhlasené pro omezený okruh uživatelů. ☐ ANO ☐ NE

5. Plán monitoringu a vyhodnocení (kdy, kdo, podle čeho rozhodne). ☐ ANO ☐ NE

6. Stop pravidlo – kdy agenta zastavíme. ☐ ANO ☐ NE

Krok, který se nejčastěji opomíjí.

Provoz a údržba

3–5 metrik se sbírá pravidelně bez velké zátěže. ☐ ANO ☐ NE

Postup pro hlášení chyby a incidentu je dostupný uživatelům. ☐ ANO ☐ NE

Plán pravidelného přehodnocení podle vytíženosti a rizika. ☐ ANO ☐ NE

Po každé změně role nebo integrace se opakují klíčové testy. ☐ ANO ☐ NE

Pravidlo: agent jde do provozu jen tehdy, když je vše výše **ANO**. Jeden chybějící bod = nedělat kompromisy, doplnit a teprve potom spustit.

