SPIES CREATIONS · LEAD-MAGNET · 2026

Tekent u nog voor wat uw AI-agent doet?

Agent-governance — de minimale set voor het MKB

AI-agents nemen steeds vaker actie in productie: orders, mails, planningen, betalingen. Goede governance betekent niet ISO/IEC 42001-certificering. Het betekent dat u op vier vragen een eenduidig antwoord kunt geven — vandaag, niet na het eerste incident.

Loop deze checklist één keer per agent door. Eén "nee" is een werkpunt. Drie "nee's" in dezelfde sectie is een live-gang-stop.

SECTIE 1 Grenzen van autonomie

Wat mag de agent zelf, en wat niet?

- ☐ Per type actie (bestellen, mailen, plannen, betalen) is op papier vastgelegd welke handelingen de agent zelfstandig mag uitvoeren.
- ☐ Voor financiële acties is een drempelbedrag bepaald waarboven menselijke goedkeuring vereist is.
- ☐ Voor acties richting klanten of leveranciers (mails, contractwijzigingen, excuusberichten) is bepaald welke handelingen langs een mens moeten.
- ☐ Er is een lijst van expliciet verboden handelingen ("nooit zonder mens") die de agent technisch niet kan uitvoeren — niet alleen omdat het in de prompt staat.
- ☐ De grenzen zijn met de relevante teams (verkoop, inkoop, finance) afgestemd en niet alleen IT-intern bedacht.

> *Geen drie vinkjes in deze sectie? Dan is een autonomie-matrix uw eerstvolgende stap.*

SECTIE 2 Audit trail — bewijs van wat de agent deed

Kunt u op een later moment nog reconstrueren wat de agent op een willekeurige eerdere dag heeft gedaan?

- ☐ Iedere actie (input, gebruikte gegevens, tool-aanroep, uitkomst) wordt opgeslagen op een plek die ook over zes maanden nog raadpleegbaar is.
- ☐ Het logboek is leesbaar voor een collega die geen ontwikkelaar is — bijvoorbeeld een operations-manager of accountant.
- ☐ Bij twijfel is binnen vijf minuten op te zoeken: wélke beslissing nam de agent, op grond van wélke informatie, om hoe laat, in opdracht van wie.
- ☐ Het logboek is beveiligd tegen onbedoelde wijziging of verwijdering door de agent zelf.
- ☐ Er is een vaste persoon (rol, niet alleen naam) verantwoordelijk voor het periodiek doornemen van het logboek.

> *Een logboek dat niemand leest is bewijs in theorie. Een vaste leesfrequentie is even belangrijk als de log zelf.*

SECTIE 3 Stop-knop en herstel

Hoe snel grijpt u in als het misgaat?

- [ ] Er is een technische pauze-knop die de agent direct stilzet (geen "we trekken wel de stekker uit de server"-improvisatie).
- [ ] Minimaal twee mensen weten waar de pauze-knop zit en hebben er toegang toe.
- [ ] Voor de meest risicovolle acties (bestelling, betaling, contractverzending) is vooraf gedocumenteerd hoe een misser wordt teruggedraaid of gecompenseerd.
- [ ] Er is afgesproken wie de klant of leverancier informeert wanneer er iets is misgegaan — en welke toon daarbij hoort.
- [ ] De stop-procedure is minstens één keer geoefend, niet alleen op papier vastgelegd.

> *Een stop-knop die u nooit heeft uitgeprobeerd is geen stop-knop. Eén realistische oefening per kwartaal volstaat voor het MKB.*

SECTIE 4 Documentatie en verantwoording

Wat ligt er als de accountant, verzekeraar of toezichthouder ernaar vraagt?

- [ ] Er bestaat een korte, leesbare beschrijving van de agent: doel, ingezet model of leverancier, datatoegang, autonomie-grenzen.
- [ ] De verantwoordelijke personen (eigenaar, technisch beheerder, intern aanspreekpunt) zijn benoemd.
- [ ] De leverancier van het onderliggende model heeft de relevante EU AI Act-documentatie beschikbaar (technische documentatie, transparantie-informatie voor GPAI).
- [ ] Bij elke significante wijziging in het gedrag van de agent (model-update, nieuwe tool, gewijzigde prompt) wordt de beschrijving bijgewerkt.

> *Per 2 augustus 2026 is de EU AI Act in brede toepassing van kracht. Voor het MKB als afnemer is "wij weten wat onze agent doet" geen wens meer, maar een uit te leggen feit.*

Volgende stap

Loopt u op één van de vier secties tegen meer dan twee onbeantwoorde punten aan? Dat is geen reden voor paniek — wel een reden om dit niet alleen op te lossen.

Wij helpen MKB-bedrijven om in een paar middagen een werkbare governance-basis neer te zetten: een autonomie-matrix, een leesbare audit trail, een geoefende stop-procedure en de documentatie die u nodig heeft. Geen ISO-traject, geen overweldigend framework — gewoon de minimale set, op uw eigen proces toegesneden.

SPARREN? **Plan een uur met Stephan — geen verkopers-script.**

Spies Creations
WordPress · Laravel · Integraties · AI-koppelingen voor MKB

stephan@spiescreations.nl
spiescreations.nl/contact

Spies Creations · KvK 57215782 · BTW NL001956622B49 · De Mulderij 4B, 3831 NV Leusden