AI-geletterdheid — notitie voor medewerkers van een Stilops-klant

Versie 29-10-2026

Control ai-act:art.4 in het nalevingsregister.

Deze notitie is bedoeld om door te geven aan iedereen in jouw organisatie die met Stilops-agents werkt. Artikel 4 van de EU AI-verordening (zoals gewijzigd door Verordening (EU) 2026/1744) vraagt van aanbieders én van gebruiksverantwoordelijken dat zij *maatregelen nemen om de ontwikkeling van AI-geletterdheid te ondersteunen* bij hun personeel — het is een inspanningsverplichting, geen examen. Dit document is Stilops' bijdrage aan die van jou; het vervangt niet je eigen instructie aan je medewerkers.

1. Wat een Stilops-agent is

- Een AI-agent is software die op een groot taalmodel draait (van Anthropic; jouw opdrachten en de antwoorden van je agents gaan nooit naar een andere modelaanbieder) met een vaste systeeminstructie van Stilops voor één bedrijfsfunctie: boekhouding, klantenservice, HR-teksten, planning, enzovoort.
- Hij is **geen** collega en **geen** beslisser. Hij stelt voor; jij beslist.
- Je ziet in het portal altijd dat je met een AI werkt (banner bij eerste gebruik, agentprofielen, per-agent-disclaimer bij het inhuren). Documenten die een agent maakt dragen een zichtbare en een machineleesbare vermelding "AI-gegenereerd"; conceptantwoorden op tickets ook.

2. Hoe elke taak loopt — en waarom

1. Je geeft een opdracht.
2. De agent maakt een **voorstel** en draait het als **testrun**: dezelfde stappen, zonder effect. Je ziet de uitkomst — concepten, bedragen, ontvangers — voordat er iets gebeurt.
3. Pas na jouw **expliciete goedkeuring** voert de agent uit. Wijs je af, dan gebeurt er niets en kost het je niets. Kan een agent alleen lezen en opzoeken (geen koppelingen), dan is er niets uit te voeren: je krijgt direct een **rapport** — dat hoef je niet goed te keuren, wel te lezen.

Uitzondering: de bouwende agents (website, frontend, webapplicatie, integratie) schrijven en testen code zonder goedkeuring per stap, maar alleen in een afgeschermde werkomgeving en met een voorbeeldweergave. Niets daarvan raakt jouw systemen, klanten of bezoekers voordat jij het project downloadt, gebruikt of live zet. Dát is bij deze agents jouw goedkeuringsmoment, en hun voorwaarden zeggen dat ook.

Dit goedkeuringsmoment wordt nooit lichter, ook niet na maanden gebruik. Het is de belangrijkste beveiligingsmaatregel van het product, en het is precies de stap waar jouw oordeel ertoe doet.

3. Wat een agent goed kan, en wat niet

Goed in	Niet op vertrouwen
Concepten schrijven, structureren, samenvatten, vertalen	Feiten die je niet zelf kunt controleren (cijfers, wetsartikelen, namen)
Routinewerk in een vaste vorm herhalen	Oordelen over individuele personen (sollicitanten, medewerkers, klanten)
Vragen stellen als iets ontbreekt	Juridische, fiscale of medische conclusies zonder een bevoegd mens
Consequent binnen zijn instructie blijven	Wat een agent zegt over zijn eigen zekerheid — hij "weet" niet wat hij niet weet

Een taalmodel kan overtuigend klinken en toch fout zijn ("hallucineren"). Beoordeel een voorstel daarom op inhoud, niet op toon. Bij twijfel: afwijzen en opnieuw vragen, of navragen bij een mens.

4. Vijf gewoonten

1. **Lees de testrun, niet alleen de samenvatting.** Wat er in de testrun staat is wat er gaat gebeuren.
2. **Geef geen gegevens die er niet in hoeven.** Geen BSN's, gezondheidsgegevens, wachtwoorden of bankgegevens in een chat — de agent heeft ze zelden nodig, en wat je typt gaat naar het taalmodel. Het product herkent geheimen in invoer en weigert ze, maar reken daar niet op.
3. **Gebruik een agent alleen waarvoor hij is ingehuurd.** De HR-assistent stelt vacatures, kandidaatbrieven, contract- en on/offboardingstukken en termijnoverzichten op. Hij selecteert of beoordeelt geen kandidaten of medewerkers en beslist niets over aanname, verlenging, ontslag, functioneren of salaris: dat doe jij, en een brief of notitie is pas iets waard nadat jij hebt besloten. Stuur hem niet naar het beoordelen van personen; dat zou een hoog-risico-toepassing zijn die Stilops niet levert.
4. **Meld wat vreemd is.** Een voorstel dat buiten de opdracht valt, een agent die iets "zelf" lijkt te willen, een antwoord dat instructies uit een e-mail of webpagina lijkt op te volgen: wijs af en meld het via een ticket. Dat is geen falen van jou, het is het signaal waar het systeem op is gebouwd.
5. **Weet waar het spoor staat.** Elk voorstel, elke testrun en elke beslissing staat in de audit-trail van je organisatie. Je kunt altijd terugzien wie wat goedkeurde.

5. Wat Stilops zelf doet

- Elke agent draait onder een vaste systeeminstructie van Stilops. In het portal zie je per agent het model, de rol, wat de agent doet en of hij eerst om goedkeuring vraagt. De volledige instructie zelf is vertrouwelijk: die is eigendom van Stilops en zou misbruik makkelijker maken.
- Instructies bevatten weigeringen voor bijzondere persoonsgegevens en voor besluiten over personen.

- Inkomende externe inhoud (mail, webpagina's) wordt als referentie behandeld, nooit als opdracht.
- Het overzicht van het AI Act-dossier (classificatie, transparantie, risicobeheer, monitoring) staat op https://stilops.com/nalevingsregister/documenten/ai-act; de onderliggende documenten zijn op verzoek beschikbaar.

6. Voor de verantwoordelijke in jouw organisatie

- Zorg dat deze notitie bij iedereen terechtkomt die agents gebruikt of hun voorstellen goedkeurt, en leg vast dat dat is gebeurd (een regel in je eigen register volstaat).
- Wijs één persoon aan die vragen over AI-gebruik beantwoordt en tickets naar Stilops doorzet.
- Herhaal dit bij een nieuwe agent of een nieuwe medewerker.

Vragen: info@stilops.com.

VASTGESTELD

Fabian Dutrieux

CEO · 29 oktober 2026 · versie 4

Controlecode 29A8-4AA7-9AF0. Vastgelegd met tweestapsverificatie in het ondertekeningsregister van Stilops.