

Instructie invullen

### Inleiding

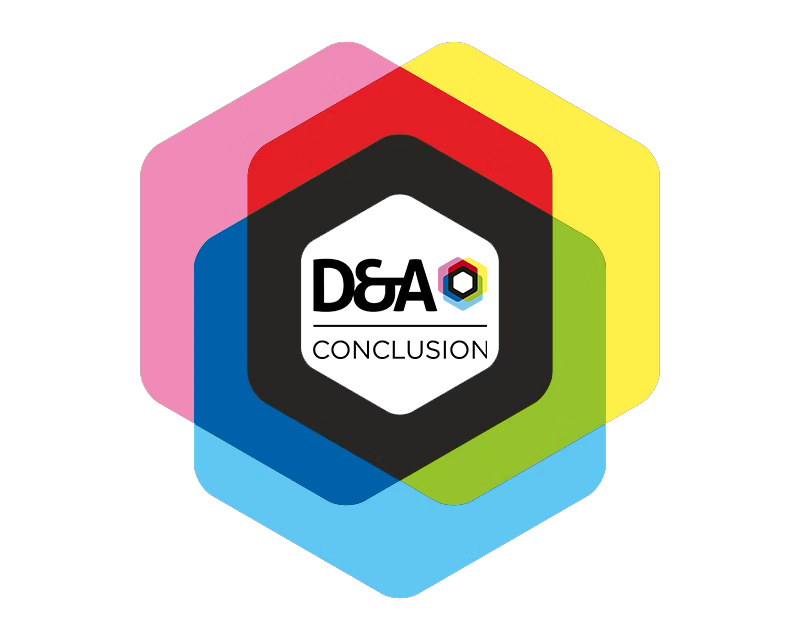
Hartelijk dank voor het opvragen van dit document. Ik hoop dat deze richtlijn u helpt bij het verantwoord inzetten van AI binnen uw zorginstelling. Hieronder vindt u enkele tips om dit document snel en efficiënt in te vullen.

### Tips voor het invullen

* Vervang alle tekst tussen blokhaken met de juiste gegevens voor uw organisatie.
* Voor een snel overzicht, hier zijn de termen die ingevuld moeten worden:
* [naam organisatie]
* [ECD/EPD naam]
* [naam juridische afdeling of juridisch contactpersoon]
* [link security documenten]
* [AI coördinator]
* [email AI coördinator]
* [telefoonnummer AI coördinator]

Als u vragen heeft of hulp nodig heeft bij het invullen, of als u vragen heeft over de implementatie van AI binnen uw organisatie en het naleven van regelgeving zoals de Europese AI-verordening, neem dan gerust contact met mij op. U kunt mij bereiken bij D&A Medical Group via michiel.tebbes@dnagroup.nl.

Kleine lettertjes  
Er kunnen geen rechten worden ontleend aan deze voorbeeldsjabloon. Deze sjabloon is niet bindend en er wordt geen garantie gegeven voor de juridische juistheid of toepasbaarheid, hoewel de ontwikkelaar uiterste zorg heeft besteed om aan de geldende juridische vereisten te voldoen. Dit document valt onder een Creative Commons-licentie ([CC BY-NC 4.0](https://creativecommons.org/licenses/by-nc/4.0/)), wat betekent dat het gedeeld en aangepast mag worden voor niet-commerciële doeleinden, mits correcte bronvermelding wordt gegeven. Om de zorg sneller AI-ready te maken vraag ik u om, als u een fout, aanvulling of verbetering vindt in dit document om dit te delen met de community.

Voorbeeld Richtlijn voor het Gebruik van Large Language Models (LLMs)

*(Afspraken in makkelijke taal staan onderaan)*

# Inleiding

De opkomst van AI gestuurde systemen zoals ChatGPT en Copilot biedt nieuwe mogelijkheden om werkprocessen te verbeteren. Deze technologieën kunnen taken ondersteunen variërend van administratieve werkzaamheden tot communicatie met patiënten. Tegelijkertijd brengen ze ethische en technische uitdagingen met zich mee, vooral op het gebied van privacy en gegevensbescherming. Het is daarom essentieel dat LLMs op een verantwoorde en zorgvuldige manier worden ingezet, met respect voor privacy, veiligheid en professionele standaarden. Deze richtlijn stelt kaders vast voor het gebruik van chatbots en LLMs binnen zowel zorg als niet-zorgprocessen, in overeenstemming met wet en regelgeving en ethische normen.

# Afstemming met Organisatiebeleid

Alle initiatieven voor het gebruik van chatbots en LLMs moeten aansluiten bij de strategische doelen en het beleid van [naam organisatie]. Dit bevordert een efficiënte inzet van middelen en voorkomt fragmentatie van inspanningen.  
Tip: Voordat je een nieuw project start met LLMs, consulteer de relevante afdelingen om te zorgen voor alignment met bestaande initiatieven en beleid.

Voorbeeld Correct Gebruik  
Een team wil een chatbot implementeren om veel gestelde vragen van patiënten te beantwoorden. Ze bespreken dit met het management en de afdeling ICT om ervoor te zorgen dat het project aansluit bij de organisatieprioriteiten en voldoen aan de veiligheidsnormen.

Voorbeeld Onjuist Gebruik  
Een individuele medewerker start op eigen initiatief een experiment met een externe LLM-dienst zonder overleg of goedkeuring. Dit kan leiden tot beveiligingsrisico's en misalignment met organisatiebeleid.

# Gebruik Binnen Niet Kritische Processen

LLMs dienen in eerste instantie te worden ingezet binnen niet kritische processen, zoals administratieve taken, klantondersteuning of interne communicatie. LLMs als Copilot of ChatGPT zijn geen ‘medical devices’ en het gebruik voor diagnostiek en behandeling is verboden.

Voorbeeld Correct Gebruik  
Een medewerker gebruikt een LLM om een interne nieuwsbrief op te stellen, waarbij hij de output controleert en aanpast voor verzending.  
  
Voorbeeld Onjuist Gebruik  
Een zorgverlener gebruikt een niet goedgekeurd LLM om automatisch patiëntverslagen te genereren en deze zonder verificatie aan het medisch dossier toe te voegen.

Tip: Vermijd het gebruik van LLMs in medische beslissingsprocessen zonder grondige testen en formele goedkeuring. De in [ECD/EPD naam] gebruikte LLM is door [naam organisatie] goedgekeurd en mag gebruikt worden.

# Bescherming van Persoonsgegevens

Het beschermen van persoonsgegevens is van het grootste belang. Er mogen geen identificeerbare gegevens van patiënten of medewerkers worden ingevoerd in LLMs, tenzij deze volledig geanonimiseerd zijn.  
Tip: Controleer altijd of gegevens volledig zijn geanonimiseerd voordat je ze invoert in een LLM.

Voorbeeld Correct Gebruik  
Een onderzoeker voert geanonimiseerde datasets in een LLM om trends te analyseren zonder dat individuele patiënten kunnen worden geïdentificeerd.

Voorbeeld Onjuist Gebruik  
Een medewerker kopieert en plakt een email met patiëntinformatie in een LLM om een reactie te genereren, waardoor persoonlijke gegevens kunnen lekken.

# Bescherming van Bedrijfsgevoelige Informatie

Vertrouwelijke bedrijfsinformatie mag niet worden gedeeld met of verwerkt door niet door [naam organisatie] goedgekeurde LLMs.  
Tip: Deel geen interne strategieën, financiële gegevens of andere gevoelige informatie met LLMs.

Voorbeeld Correct Gebruik   
Een medewerker vraagt een LLM om algemene adviezen over timemanagement zonder specifieke bedrijfsinformatie te delen.

Voorbeeld Onjuist Gebruik  
Een manager voert gedetailleerde interne financiële rapporten in een LLM in om een presentatie te laten genereren.

# Professionele Controle en Verantwoordelijkheid

LLMs zijn hulpmiddelen en geen vervanging voor professionele expertise. De eindverantwoordelijkheid ligt altijd bij de menselijke professional.  
Tip: Controleer en valideer altijd de output van een LLM voordat je deze gebruikt of deelt.

Voorbeeld Correct Gebruik  
Een arts gebruikt een LLM om een complex medisch concept in lekenbegrippen uit te leggen en verifieert de uitleg voordat deze aan de patiënt wordt gegeven.

Voorbeeld Onjuist Gebruik  
Een arts vertrouwt op een LLM voor medicatiedoseringen zonder deze te controleren, wat kan leiden tot medicatiefouten.

# Naleving van Wet en Regelgeving

Alle toepassingen van LLMs moeten voldoen aan nationale en internationale wet en regelgeving, zoals de Algemene Verordening Gegevensbescherming (AVG), Medical Device Regulation (MDR), Wet op de Geneeskundige Behandel Overeenkomst (WGBO).  
Tip: Raadpleeg [naam juridische afdeling of juridisch contactpersoon] bij twijfel.

# Veiligheid en Beveiliging

Gebruik uitsluitend door [naam organisatie] goedgekeurde platforms en diensten voor LLMs. Vermijd het gebruik van openbare en/of onbeveiligde systemen.  
Tip: Zorg ervoor dat alle gebruikte systemen voldoen aan de IT-beveiligingsnormen van [naam organisatie]. Meer informatie over de beveiligingsnormen kan je hier vinden [link security documenten]

Voorbeeld Correct Gebruik  
Een medewerker gebruikt een intern goedgekeurde LLMdienst die voldoet aan alle veiligheidsprotocollen.

Voorbeeld Onjuist Gebruik  
Een medewerker gebruikt een gratis online LLMtool voor het verwerken van gevoelige informatie zonder te verifiëren of deze veilig is.

# Training en Bewustwording

Medewerkers moeten worden getraind in het verantwoord gebruik van LLMs en zich bewust zijn van de risico's en beperkingen.  
Tip: Neem deel aan trainingssessies en blijf op de hoogte van best practices.

Voorbeeld Correct Gebruik  
Een medewerker volgt een training over het gebruik van LLMs en past de geleerde principes toe in zijn dagelijkse werk.

Voorbeeld Onjuist Gebruik  
Een medewerker is zich niet bewust van de risico's en gebruikt een LLM op een manier die in strijd is met de organisatiebeleid.

# Monitoring en Evaluatie

Het gebruik van LLMs moet regelmatig worden gemonitord en geëvalueerd om naleving en effectiviteit te waarborgen.  
Advies: Documenteer het gebruik van LLMs en ander AI applicaties en maak dit een vast onderdeel van de management agenda.

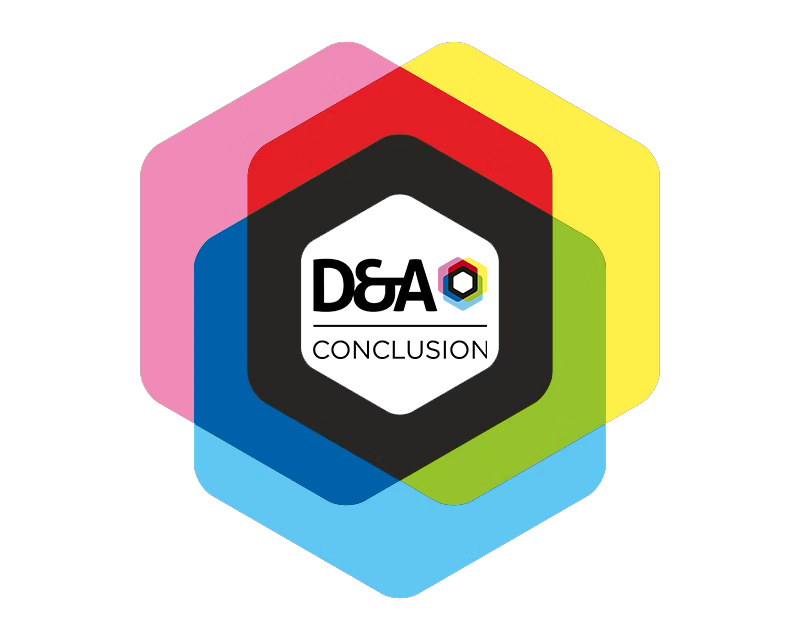
# Algemene Tips voor het Gebruik van LLMs

Voor optimale resultaten bij het gebruik van LLMs:

* Beschrijf het Publiek: Wie is de doelgroep?
* Specificeer het Taalniveau: Wat is het opleidingsniveau of begrip van de doelgroep?
* Omschrijf het Doel: Wat wil je bereiken met de output?
* Vorm en Stijl: In welke vorm moet de output worden gepresenteerd?
* Beperkingen: Geef duidelijke instructies over lengte en scope.
* Gebruik LLMs als Taalhulpmiddelen, Niet als Kennisbronnen.

# Contact en Innovatie

Voor vragen over LLM’s of ideeën om nieuwe toepassingen te verkennen, neem contact op met [AI coördinator], [email AI coördinator]/ [telefoonnummer AI coördinator]. Deze afdeling kan je verder helpen bij de ontwikkeling en implementatie van AI-projecten.

Afspraken over het Gebruik van Slimme Computers

Slimme computers zoals ChatGPT en Copilot maken het werk makkelijker. Ze kunnen helpen met taken zoals vragen beantwoorden en teksten schrijven. Maar er zijn ook zorgen over privacy en veiligheid. Daarom moeten we deze computers voorzichtig en volgens de regels gebruiken.

# Gebruik binnen [naam organisatie]

Als je een project met een slimme computer wilt starten, zorg dan dat het past bij de doelen van de organisatie. Overleg altijd met je manager als je wilt starten met gebruiken van slimme computers. Zo voorkom je misverstanden en werk je veilig.

# Waar te gebruiken?

Gebruik slimme computers voor niet-kritische taken, zoals administratief werk of klantenservice. Gebruik ze niet voor medische beslissingen als ze niet goed getest en goedgekeurd zijn. Voor minder belangrijke taken, zoals het schrijven van een nieuwsbrief, kun je ze wel gebruiken. Lees altijd het antwoord van de slimme computer. Ze kunnen ook fouten maken.

# Bescherming van gegevens

Het is belangrijk om gegevens te beschermen bij het gebruik van slimme computers. Voer geen persoonlijke informatie in, zoals namen of medische gegevens, tenzij ze helemaal anoniem zijn. Dat betekent dat niemand kan zien over wie het gaat. Deel ook geen andere vertrouwelijke informatie met slimme computers.

# Veiligheid en beveiliging

Gebruik alleen slimme computers die door [naam organisatie] zijn goedgekeurd. Openbare of onbeveiligde computers zijn niet veilig voor vertrouwelijke informatie. Alle systemen moeten voldoen aan de veiligheidsregels van [naam organisatie].

# Verantwoordelijkheid

Hoewel slimme computers helpen, blijft de mens verantwoordelijk. Een slimme computer is een hulpmiddel, maar je moet altijd zelf beslissen en de resultaten controleren. Bijvoorbeeld: een arts kan een slimme computer gebruiken om iets uit te leggen, maar moet altijd controleren of het klopt voordat zij het aan een patiënt vertelt.

# Wetgeving en naleving

Alles wat je met slimme computers doet, moet volgens de wet zijn. Ze moeten werken volgens regels zoals de privacywet. Als je twijfelt, neem dan contact op met [AI coördinator], [email AI coördinator] / [telefoonnummer AI coördinator].

# Training en bewustzijn

Het is belangrijk dat je leert hoe je slimme computers veilig en goed kan gebruiken. Daarvoor hebben wij als [naam organisatie] een cursus die je gratis kan volgen.

# Controle en evaluatie

Het gebruik van slimme computers moet regelmatig worden gecontroleerd en beoordeeld. Zo kun je zien of alles volgens de regels gaat en of de computers goed werken. Op deze manier kunnen we als [naam organisatie] slimme computers veilig en nuttig inzetten.

Vragen of Ideeën  
Als je vragen of ideeën hebt hoe slimme computers jou werk makkelijker kunnen maken praat er over met je leidinggevende of met [AI coördinator], [email AI coördinator] / [telefoonnummer AI coördinator].

# Moeilijke woorden

**AI (Kunstmatige Intelligentie)**: Slimme computers die dingen kunnen doen zoals mensen, bijvoorbeeld vragen beantwoorden.  
**ChatGPT en Copilot**: Voorbeelden van slimme computers die teksten schrijven en begrijpen.  
**LLM (Large Language Model)**: Een slimme computer die veel tekst kan begrijpen en maken.  
**Niet-kritische processen**: Taken die niet heel belangrijk zijn, zoals administratie.  
**Ethische uitdagingen**: Vragen over wat goed of fout is bij het gebruik van technologie.  
**Gegevensbescherming**: Het veilig bewaren van persoonlijke informatie, zodat anderen het niet kunnen zien of gebruiken.  
**Persoonsgegevens**: Informatie over een persoon, zoals naam, adres of gezondheidsgegevens.  
**Anonimiseren**: Persoonsgegevens zo veranderen dat niemand kan zien van wie ze zijn.  
**Bedrijfsgevoelige informatie**: Geheime informatie over een bedrijf die niet mag worden gedeeld.  
**Beveiliging**: Het beschermen van gegevens zodat niemand er zonder toestemming bij kan.  
**Professionele verantwoordelijkheid**: De plicht om werk goed te doen.  
**Wet en regelgeving**: Regels en wetten waar iedereen zich aan moet houden, zoals de privacywet.  
**Compliance**: Het volgen van regels en wetten in je werk.  
**Monitoring**: Het controleren of iets goed gaat.  
**Evaluatie**: Kijken of iets goed werkt of beter kan.