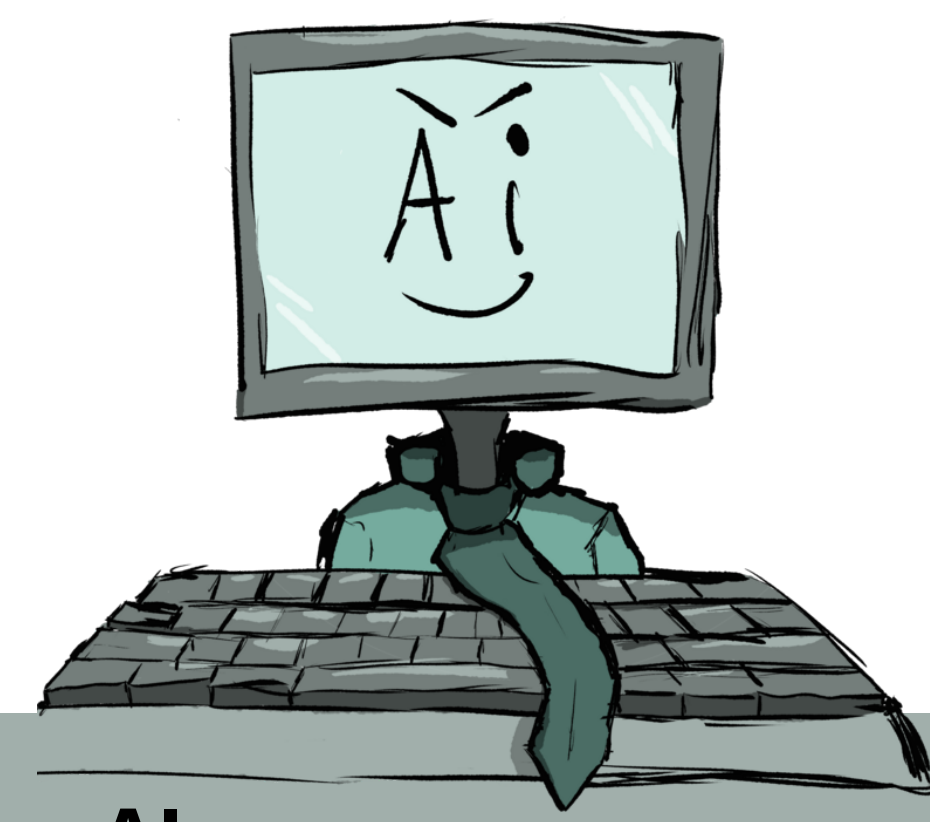




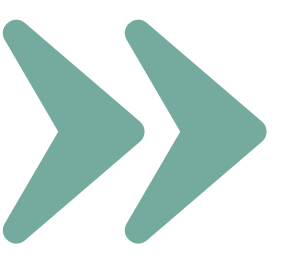
Hoe werkt generatieve AI

Generatieve AI, zoals ChatGPT, gebruiken de data die je invoert om hun systeem te onderhouden en verbeteren. Dit betekent dat de vragen die jij stelt, maar ook de teksten die je invoert, gebruikt worden. Veel bedrijven achter generatieve AI zijn uit landen buiten de EU. Dit betekent dat als jij gegevens over jezelf of een ander invoert, deze persoonsgegevens gedeeld worden met deze bedrijven. Zij delen vaak ook weer gegevens met andere bedrijven.



Meer over generatieve AI

AI-chatbots zijn taalmodellen. Ze zijn getraind om grammaticaal goede zinnen te maken. Ze kunnen niet inschatten wat waar is en wat niet. Wees voorzichtig met wat je gelooft en check de bronnen. AI-chatbots hebben ook een kwaal genaamd "hallucineren". Hierbij lijkt de AI-chatbot zelf informatie te verzinnen omdat dit taalkundig een logische volgende zin is. Een andere kwaal is "cognitive biases". Dit zijn vooroordelen. Veel chatbots zijn getraind op voornamelijk westerse data. Dit kan ervoor zorgen dat de vooroordelen die in de trainingdata zitten worden overgenomen door de AI-chatbot.



Verstandig gebruik: waarom

Je mag niet zomaar informatie over jezelf of een ander invoeren. Dit geldt ook voor bedrijfs-vertrouwelijke gegevens (bijvoorbeeld over de financiële positie van of processen in de organisatie) en intellectueel eigendom. Het kán leiden tot het lekken van vertrouwelijke informatie. Dit is een reden dat organisaties, zoals multinationals en de Rijksoverheid, en ook de HU, het gebruik van ChatGPT niet toestaan. Een organisatie hoort namelijk eerst afspraken te maken met bedrijven achter de generatieve AI systemen en dat kan met de meeste bedrijven nog niet.



Verstandig gebruik: hoe

Gebruik de juiste tool

Controleer of je bij je opdracht AI-chatbots mag gebruiken. Als dat mag, maak dan gebruik van de tool die de HU adviseert, momenteel is dit Copilot Enterprise Data Protection. Je vindt deze tool als je inlogt met je HU-account. Check bij je stage-afstudeer- of praktijkorganisatie welke AI-tools je mag gebruiken, wellicht hebben zij iets anders ingericht dan Copilot Enterprise Data of verbieden zij het gebruik van Copilot Enterprise Data.

Zo werk je met Copilot Enterprise (EDP)

- Ga naar [Copilot.microsoft.com](https://copilot.microsoft.com) en log in met je HU-account. Hoe controleer je dat je bent ingelogd met je eigen account en de data dus binnen de HU blijft? Kijk of je boven in je scherm een groen schildje ziet en  jouw eigen profielfoto rechtsboven.
- Deel bij het gebruik geen persoonsgegevens, vertrouwelijke gegevens of bedrijfsgegevens.
- Sta stil bij de betrouwbaarheid van het resultaat dat je ontvangt. Blijf kritisch.

Deel geen vertrouwelijke gegevens (waaronder persoonsgegevens)

Als je een AI-chatbot mag gebruiken, zet dan geen persoonsgegevens of andere vertrouwelijke informatie in de prompts (de opdracht aan de chatbot). Deel dus geen namen maar ook geen teksten met persoonlijke informatie over je gezondheid, financiële informatie over een organisatie, ervaringen met je stage, cliënten etc. Vraag AI-chatbots niet om zich voor te doen als bestaande personen of bedrijven. Het kunnen dan nog steeds persoonsgegevens zijn en het kan zelfs leiden tot smaad. Verder, als je het mag gebruiken als student, verwijst er dan naar zoals de docent aangeeft. Er is al een APA-stijl ontwikkeld die je kunt gebruiken. Het kan ook zijn dat een docent je vraagt om screenshots van je prompts en de antwoorden van een generatief AI-systeem bij je opdracht te voegen.

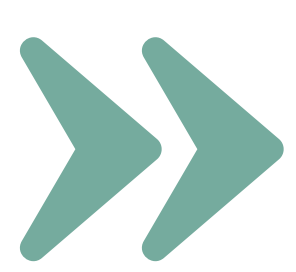


Toekomst

De HU blijft de ontwikkelingen en de onderzoeken naar de veiligheid van AI-tools (bijv. door SURF) volgen en zal hierop ook besluiten over de inzet van AI. Blijf het nieuws hierover dus volgen! Ook zal het in de toekomst mogelijk zijn om zelf getrainde AI-chatbots in een afgesloten omgeving te maken en te gebruiken, zie voor informatie hierover het AI Proeflokaal (aiproeflokaal.nl).

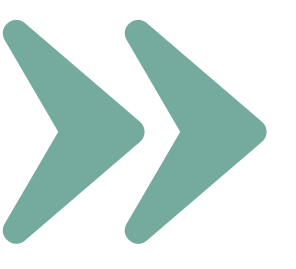
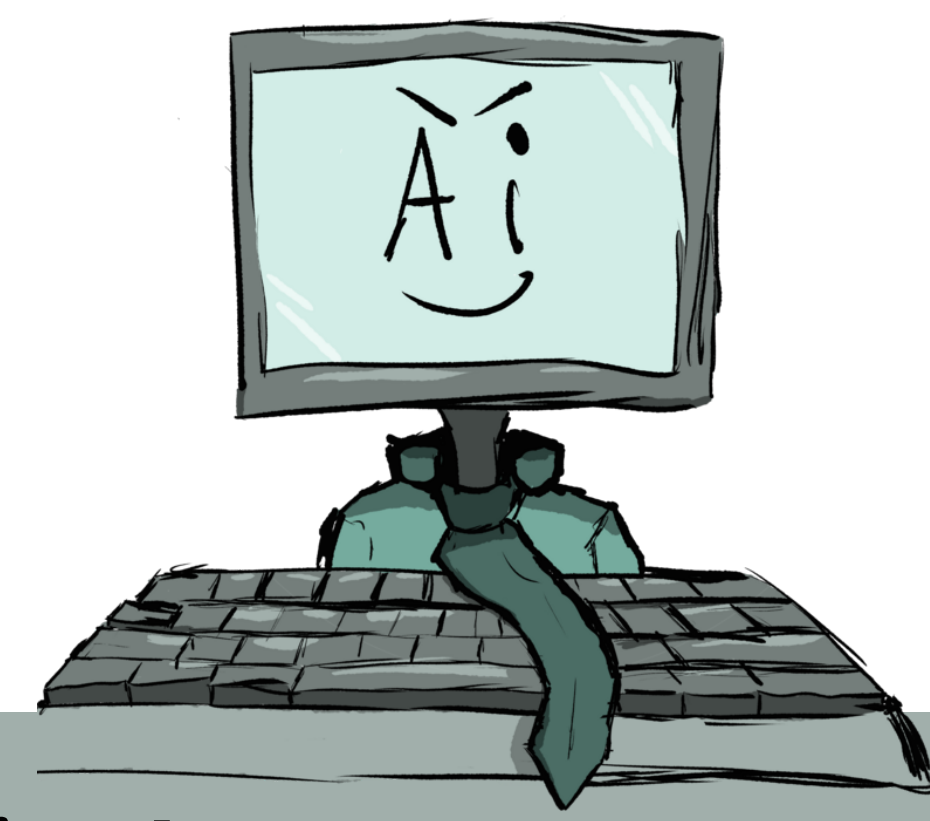
KENNISWERKPLAATS
ZORGVULDIG DATA DELEN
I:U VEILIGHEIDSLAB

Deze informatie is opgesteld door de Kenniswerkplaats Zorgvuldig Data Delen van Hogeschool Utrecht. Versie maart 2025. Voor meer informatie kunnen studenten en docenten contact opnemen met de privacy officer van hun instituut. Docenten hebben toegang tot de Handreiking generatieve AI en toetsing - via Eén HU.



AI: how does it work

Generative AI, like ChatGPT, uses the data you enter to maintain and improve its system. This means using the questions you ask and the texts you enter. Many of the companies behind generative AI are American or from countries outside the EU. This means that when you enter data about yourself or another person, this personal data is shared with the companies behind the generative AI system. In turn, these companies often share data with other companies.



Use wisely: why

You should not enter personal information about yourself or another person. If you work with company confidential data (e.g. about the financial position or processes in the organisation) and intellectual property, using generative AI like ChatGPT can lead to the leakage of confidential information. This is one reason organisations, such as multinationals and the central government, and also HU, do not allow ChatGPT. An organisation should arrange data processing agreements with companies behind the generative AI systems. At this moment, this is only possible with some generative AI companies.

More about generative AI

AI chatbots are language models. They are trained to make grammatically sound sentences. However, AI chatbots cannot judge what is true and what is not. Be careful what you believe and check sources. AI chatbots "hallucinate." The AI chatbot seems to make up its own information to come to a linguistically logical next sentence. AI chatbots also suffer from "cognitive biases." Many AI chatbots are trained on mainly Western data, which can cause biases in the training data that the AI chatbot adopts.



Use wisely: how

Use the right tool

Check if you are allowed to use AI chatbots for your assignment. If so, use the tool recommended by HU, which is currently Copilot Enterprise Data Protection. You can find this tool by logging in with your HU account. Check with your internship, graduation, or practical organization which AI tools you are allowed to use, as they may have set up something different than Copilot Enterprise Data or may prohibit the use of Copilot Enterprise Data.

How to work with Copilot Enterprise (EDP)

Go to [Copilot.microsoft.com](https://copilot.microsoft.com) and log in with your HU account.

- How do you check that you are logged in with your own account and that the data remains within HU? Look for a green shield at the top of your screen and your own profile picture in the top right corner. 
- Do not share personal data, confidential information, or company data when using it.
- Consider the reliability of the result you receive. Stay critical.

Do not share confidential information (including personal data)

If you are allowed to use an AI chatbot, do not include personal data or other confidential information in the prompts (the instructions to the chatbot). So, do not share names or texts with personal information about your health, financial information about an organization, experiences with your internship, clients, etc.

Do not ask AI chatbots to impersonate existing people or companies. This can still be considered personal data and it might result in slander.

Furthermore, if you are allowed to use it as a student, refer to it as indicated by the lecturer. An APA style has already been developed that you can use. It is also possible that a lecturer may ask you to include screenshots of your prompts and the responses from a generative AI system with your assignment.



Future

HU continues to monitor developments and research on the safety of AI tools (e.g., by SURF) and will make decisions about the use of AI based on this. So, keep following the news on this! In the future, it will also be possible to create and use self-trained AI chatbots in a closed environment. For more information, see the AI Proeflokaal (aiproeflokaal.nl).

KENNISWERKPLAATS
ZORGVULDIG DATA DELEN
I:U VEILIGHEIDSLAB