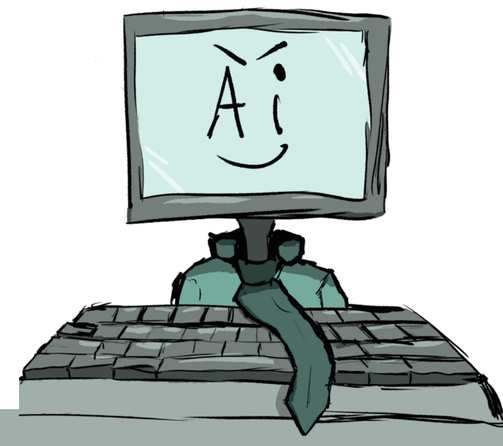
For English see below

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 bedrijfsvertrouwelijke 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

Controleer of je bij je werk of opdracht AI-chatbots mag gebruiken. Als je het mag gebruiken, zet er dan geen persoonsgegevens of andere vertrouwelijke informatie in. 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, verwijs 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 komende tijd zullen er meer organisaties zijn die contracten afsluiten met bedrijven die generatieve AI-systemen leveren waarbij alle input wél beschermd is. Binnen de HU gaan we met Microsoft Copilot werken. Als een organisatie dit geregeld heeft, dan mag je vaak wel generatieve AI gebruiken. Log dan in op het organisatienetwerk / -systeem. Want als je erbuiten werkt, dan lek je alsnog persoonsgegevens en vertrouwelijke informatie. Zie: een.hu.nl/actueel/hu-nieuws/ga-voor-veilig-gebruik-copilot-in-plaats-van-chatgpt-of-andere-ai-tool

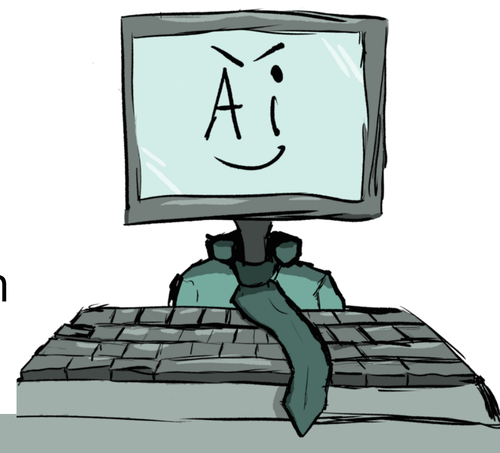
Meer informatie

Voor meer informatie kunnen studenten contact opnemen met hun docenten of de privacy officer van hun instituut. Docenten kunnen meer informatie vinden op Handreiking generatieve AI en toetsing - Onderwijs & Onderzoek (hu.nl)

Deze informatie is opgesteld door de Kenniswerkplaats Zorgvuldig Data Delen van Hogeschool Utrecht. Versie september 2024.

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.



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: 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.

Use wisely: how

Check whether you can use AI chatbots for your work or assignment; if so, do not enter personal data or other confidential information. So do not share names, but also do not share texts with personal information about your health, financial information about an organisation, experiences with your internship, clients, etc. Do not ask ChatGPT to pretend to be an existing company or a living individual. The information would still be personal data, and it might result in slander.

Also, if you are a student and you can use it, refer to it as directed by the lecturer. There is already an APA style for references to generative AI. A lecturer may also ask you to attach screenshots of your prompts and answers from a generative AI system to your assignment.

Future

More organisations will agree with companies that provide generative AI systems to protect all input. If an organisation has arranged this, you are often allowed to use generative AI if you are logged into the organisation's network and system. The HU will make Microsoft Copilot available within the coming months. If you work outside the organisation's network, you will still leak personal data and confidential information.

More information

Students can contact their lecturers or their institute's privacy officer for more information. Lecturers can find more information here: Handreiking generatieve AI en toetsing - Onderwijs & Onderzoek (hu.nl)

This information is composed by the Kenniswerkplaats Zorgvuldig Data Delen at Hogeschool Utrecht. Version September 2024.