Google Translate, ChatGPT en andere AI-diensten: de risico's

5.1.2e

3 minuten leestijd

Even een tekst vertalen met Google Translate? ChatGPT vragen om een socialmediabericht of programmacode voor je te schrijven? Het is je vast niet ontgaan dat de ontwikkelingen rondom kunstmatige intelligentie (AI) in een stroomversnelling zitten. Diensten die gebruikmaken van AI werken met de dag sneller en makkelijker. Dat is handig, maar je moet ook voorzichtig zijn. We vertellen je wat de risico's zijn. En wat wel en wat niet mag als je voor je werk dit soort diensten gebruikt.

Google Translate

De gratis vertaalservice van Google is niet altijd nauwkeurig en betrouwbaar. Verder worden de data die je invoert in Google Translate (en in bijvoorbeeld Google Lens of Google Maps) geïndexeerd en dus impliciet gepubliceerd. En ook van jou als gebruiker worden bij het gebruik ervan allerlei data opgeslagen. Interne RIVM-informatie mag je daarom *nooit* door Google Translate of een vergelijkbare vertaaldienst laten vertalen.

Wil je een tekst laten vertalen? Dan kun je gemakkelijk zelf het vertaalbureau inschakelen. Lees hier hoe: Veel gestelde vragen vertaaldiensten (EffectiefCommuniceren.Veel gestelde vragen vertaaldiensten) - XWiki (rivm.nl)

ChatGPT

Teksten die zijn gegenereerd door ChatGPT of vergelijkbare Large Language Models (LLM's), zoals Bard van Google, zijn niet altijd betrouwbaar en inhoudelijk juist. Daarnaast worden gegevens die je er invoert (net als jouw persoonsgegevens en 'tracking data') gedeeld met (in het geval van ChatGPT) Microsoft op servers in de Verenigde Staten. De privacy-risico's bij het gebruik van bijvoorbeeld ChatGPT zijn dus groot.

Om deze reden hebben we het beleid over Generatieve AI ontwikkeld. Kortgezegd mag er geen gebruik gemaakt worden van open versies van GenAI-

modellen, zoals ChatGPT in verband met de risico's op het gebied van privacy, informatiebeveiliging en vertrouwelijkheid. Wel kan er gebruik worden gemaakt van door RIVM gecontracteerde Gen AI: Microsoft OpenAI op MS Azure.

Wil je gebruik maken van de gecontracteerde AI of heb je wensen met betrekking tot het contracteren van andere dan de nu beschikbare Gen AI modellen? Neem dan contact op met innovatiemanager [redacted 5.1.2e]@rivm.nl.

Meer informatie over Generatieve AI en het beleid vind je hier.

Waarmee je rekening moet houden bij het gebruik van AI-diensten:

- Data die je invoert, wordt gebruikt om het model te trainen. Je data kan daardoor 'lekken'.
- Als je een account wilt aanmaken, mag je hiervoor geen RIVM-e-mailadres gebruiken. Gebruik ook geen wachtwoord dat je al op je werk gebruikt.
- Voer geen persoonsgegevens of andere privacygevoelige informatie in.
- Voer geen bedrijfsgegevens in (alles wordt geanalyseerd).
- De algoritmes zijn niet nauwkeuring en kwetsbaar voor beïnvloeding. Er kan foute data worden ingevoerd en dat kan leiden tot foute antwoorden.
- Pas op voor plagiaat. ChatGPT bijvoorbeeld kan tekst genereren die (ongeveer) gelijk is aan al bestaande tekst van andere auteurs.
- Data die je invoert worden vaak opgeslagen op servers in het buitenland.
- Voor gegevens die met bijvoorbeeld ChatGPT zijn gedeeld, kunnen we de bewaartermijn niet meer garanderen.

Meer weten?

Wil je meer weten over de risico's of heb je al veel gebruik gemaakt van deze diensten en wil je weten of je daardoor nu risico loopt? Neem contact op met het Onderzoeks- en Dataloket, via onderzoeksendataloket@rivm.nl.

Voor meer informatie over internationale communicatie zie: Internationale communicatie (Internationalecommunicatie.WebHome) - XWiki (rivm.nl)

Heb je vragen over informatiebeveiliging? Stuur dan een mail naar ib@rivm.nl.

Lees ook:

- Gebruik van cloudopslagdiensten, doe het niet | INsite (rivm.nl)
- Side bar in Microsoft Edge vanaf 7 april niet meer beschikbaar | INsite (rivm.nl)