

Autoriteit Persoonsgegevens waarschuwt voor risico's bij AI-chatbots en datalekken

Met de opkomst van AI-chatbots zoals ChatGPT en Copilot zien steeds meer bedrijven de voordelen van het automatiseren van klantcommunicatie en interne processen. Deze AI-chatbots kunnen gesprekken voeren, vragen beantwoorden en zelfs complexe documenten samenvatten. Hoewel deze technologie aanzienlijke voordelen biedt, brengt het ook risico's met zich mee, vooral als het gaat om de bescherming van persoonsgegevens. Wanneer medewerkers persoonsgegevens invoeren in een AI-chatbot, kan dit leiden tot ernstige datalekken.

Chatbots en hun risico's

De Autoriteit Persoonsgegevens (AP) heeft de afgelopen tijd meerdere meldingen ontvangen van datalekken die zijn veroorzaakt door het onbedoeld delen van persoonsgegevens via AI-chatbots. Dit benadrukt het risico van deze technologie, vooral wanneer medewerkers AI-tools op eigen initiatief gebruiken zonder dat zij de mogelijke gevolgen volledig begrijpen. Hoewel chatbots veel tijd kunnen besparen en repetitieve taken kunnen automatiseren, kunnen ze ook leiden tot privacy schendingen wanneer gebruikers niet goed geïnformeerd zijn over de risico's van het invoeren van persoonsgegevens.

Een belangrijk probleem is dat AI-chatbots in het algemeen niet zijn ontworpen om veilig om te gaan met gevoelige informatie. Veel bedrijven die AI-chatbots aanbieden slaan de ingevoerde gegevens op voor analyse en verbetering van hun diensten. Dit betekent dat de ingevoerde in-

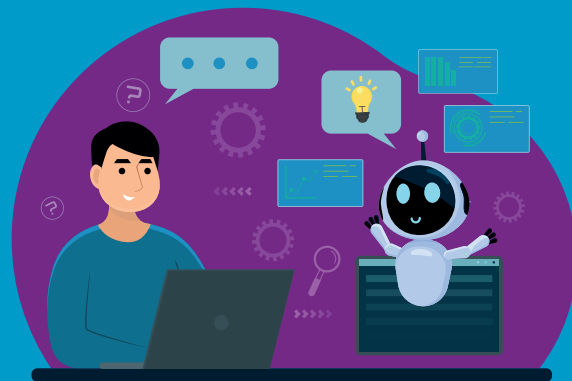
formatie, waaronder persoonsgegevens en vertrouwelijke bedrijfsgegevens, buiten de controle van de organisatie terecht kan komen. Hierdoor kunnen gegevens in handen van onbevoegden vallen zonder dat de betrokkenen, degenen die het onderwerp van de gegevens zijn, zich hiervan bewust zijn. Dit wordt een datalek genoemd.

Een datalek (zoals benoemd in de AVG-wetgeving) doet zich dus voor, wanneer er toegang is tot persoonsgegevens, zonder dat dit mag of de bedoeling is. Een datalek vormt een groot risico voor de privacy- en gegevensbescherming van zowel klanten als medewerkers.

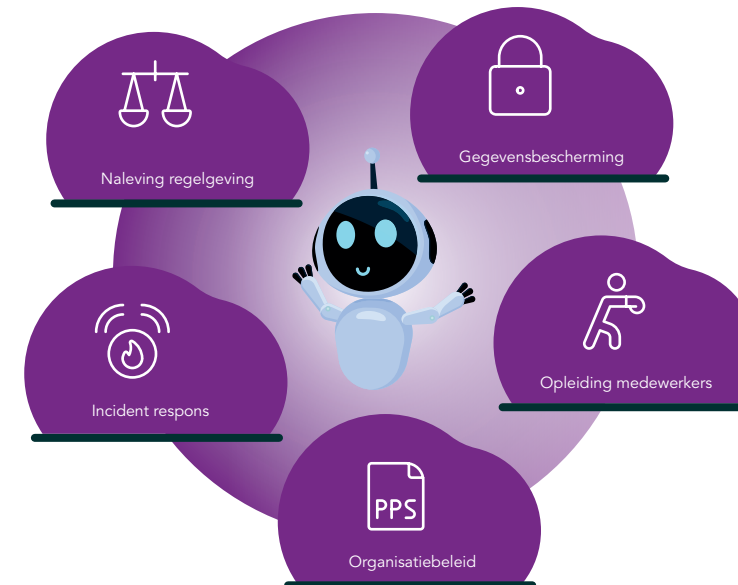
In sommige gevallen kan het gebruik van AI-chatbots onderdeel zijn van het beleid van een organisatie. Hoewel het verwerken van persoonsgegevens in AI-chatbots dan volgens de spelregels van de organisatie gaat, is het

Wat is een chatbot?

Een chatbot is een computerprogramma dat via tekst of spraak interacteert met gebruikers en gebruikmaakt van kunstmatige intelligentie (AI) om natuurlijke gesprekken te voeren. Geavanceerde AI-chatbots, zoals ChatGPT, kunnen niet alleen eenvoudige vragen beantwoorden, maar ook complexe taken uitvoeren, zoals het schrijven van teksten, analyseren van data, vertalen, en zelfs het geven van strategisch advies. Deze bots leren voortdurend bij door interactie, waardoor ze steeds beter inspelen op de behoeften van gebruikers.



Waarborgen risico's AI-chatbot



gebruik van dergelijke tools vaak nog steeds niet wettelijk toegestaan. Het is van groot belang dat organisaties beide situaties voorkomen om de privacy van hun klanten en medewerkers te beschermen.

Voorbeelden van datalekken

De AP heeft concrete datalekken geanalyseerd die voortkwamen uit het gebruik van AI-chatbots.

- **Huisartsenpraktijk**
Een van de meest opvallende gevallen betrof een huisartsenpraktijk, waar een medewerker medische gegevens van patiënten invoerde in een AI-chatbot. Medische gegevens zijn gegevens over iemands gezondheid. De AVG ziet deze gegevens als bijzondere persoonsgegevens. De AVG onderscheidt bijzondere categorieën van persoonsgegevens van gewone persoonsgegevens, omdat de verwerking van bijzondere persoonsgegevens een grote impact kan hebben op iemands leven.
- **Telecombedrijf**
In een ander geval voerde een medewerker van een telecombedrijf klantadressen in een AI-chatbot in. Hoewel de medewerker zich hier niet van bewust was, werden er hierdoor zonder rechtsgrond persoonsgegevens verstrekt aan onbevoegden.

Als er onvoldoende bewustwording is en medewerkers niet volgens de regels handelen, kunnen zelfs eenvoudige taken zoals het beantwoorden van vragen of het samenvatten van informatie tot datalekken leiden. Dit kan verstrekking van gegevens hebben, zoals identiteitsdiefstal, misbruik van persoonlijke informatie en reputatieschade voor het bedrijf.

Duidelijke afspraken binnen organisaties

Om datalekken te voorkomen, is het belangrijk dat organisaties duidelijke en strikte afspraken maken over het gebruik van AI-chatbots. Ten eerste moeten bedrijven specificeren welke gegevens wel en niet mogen worden ingevoerd in AI-chatbots. De meest veilige optie is om geen (direct of indirect herleidbare) persoonsgegevens in te voeren in ChatGPT. Als de organisatie dan toch persoonsgegevens via AI-chatbots wil verwerken, dan moeten er extra maatregelen worden getroffen om de informatie te beveiligen.

Daarnaast is het belangrijk dat medewerkers regelmatig bewust worden gemaakt in het veilig gebruik van AI-technologieën.

Medewerkers moeten weten wat de risico's zijn van het invoeren van gegevens in AI-chatbots, zodat zij kunnen voorkomen dat er persoonsgegevens in handen van onbevoegden vallen.

Deze bewustwording kan helpen om de risico's van datalekken aanzienlijk te verkleinen. Door duidelijk te communiceren over wat wel en niet is toegestaan, kunnen organisaties een cultuur van voorzichtigheid en zorgvuldigheid creëren rond het gebruik van AI-chatbots.

Toezicht en controle

Het opstellen van beleid en afspraken alleen is niet voldoende. Organisaties moeten ook toezicht houden op het gebruik van AI-chatbots en ervoor zorgen dat medewerkers zich aan de opgestelde regels houden. Dit kan betekenen dat er regelmatig gemonitord moet worden en/of audits moeten worden uitgevoerd om te controleren of medewerkers de richtlijnen volgen en of er eventuele datalekken zijn geweest.

Lees verder pagina 12

Dit soort controles helpt niet alleen om fouten te identificeren, maar geeft ook inzicht in de mate waarin AI-chatbots veilig worden gebruikt binnen de organisatie. Door regelmatig toezicht te houden en medewerkers verantwoordelijk te houden voor hun gebruik van AI-chatbots, kunnen organisaties het risico op datalekken verder verkleinen. Daarnaast is het belangrijk dat organisaties snel kunnen reageren als er toch iets misgaat. Als er bijvoorbeeld een incident plaatsvindt waarbij persoonsgegevens zijn gedeeld via een AI-chatbot, moet de organisatie direct actie ondernemen om de schade te beperken.

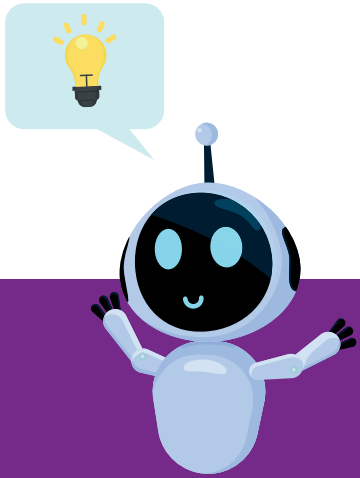
Tijdige melding van datalekken

Wanneer er een datalek optreedt, zijn organisaties in veel gevallen verplicht om dit te melden aan de AP en de getroffen personen. De AVG schrijft voor dat datalekken binnen 72 uur moeten worden gemeld aan de toezichthoudende autoriteiten. Dit geeft de betrokkenen de kans om maatregelen te nemen om hun privacy te beschermen, zoals het veranderen van wachtwoorden of het blokkeren van toegang tot gevoelige informatie. Tijdige melding van een datalek is cruciaal om verdere schade te voorkomen. Door transparant te zijn over datalekken en snel te handelen, kunnen organisaties ook hun reputatie beschermen. Hoewel datalekken altijd vervelende situaties zijn, kan een open en eerlijke benadering helpen om het vertrouwen van klanten en medewerkers terug te winnen. Organisaties die proactief en transparant zijn over het melden van datalekken, laten zien dat ze de bescherming van persoonsgegevens serieus nemen en bereid zijn om verantwoordelijkheid te nemen voor eventuele fouten.

Samenvatting

AI-chatbots zijn een krachtige tool om processen te stroomlijnen en klantcommunicatie te verbeteren. Toch brengen ze risico's met zich mee, zoals datalekken die de privacy van klanten kunnen schaden. Met duidelijke richtlijnen, goed geïnformeerde medewerkers en regelmatig toezicht kunnen organisaties deze risico's minimaliseren.

Mocht het toch misgaan, dan is snelle en transparante actie essentieel om vertrouwen te behouden. Door daarbij een balans te vinden tussen innovatie en privacy-bescherming kunnen bedrijven op een veilige manier profiteren van de mogelijkheden die AI-chatbots bieden.



Tips

- Maak een duidelijk beleid en duidelijke afspraken over het gebruik van AI-chatbots.
- Zorg voor regelmatige en gerichte training van medewerkers.
- Breng medewerkers op de hoogte van alle risico's om veiligheid en bewustzijn te vergroten.
- Voer regelmatig monitoring en audits uit om te controleren of medewerkers de interne en externe richtlijnen naleven.

Wat te doen bij een incident

- Snel en transparant reageren.
- Tijdig melden van datalekken aan de AP en de betrokkenen (binnen 72 uur).

Audit Privacy- en Gegevensbescherming

Bij InAudit begrijpen we het belang van privacy en het naleven van regelgeving zoals de Algemene Verordening Gegevensbescherming (AVG). Onze privacy- en gegevensbeschermingsaudit helpt uw organisatie om risico's te identificeren en te beheersen. Wij beoordelen uw dataverwerkingsprocessen, controleren of uw systemen voldoen aan privacywetgeving en analyseren mogelijke risico's op datalekken.

Wij zijn er om u te helpen!

