VGA
LAW & ADR

WHITE PAPER
AI COMPLIANCE

Belangrijker dan ooit

+32 11 281 280

www.vga.law

DE IMPLEMENTATIE VAN AI-TOOLS OP DE WERKVLOER

In de afgelopen jaren is een exponentiële groei waar te nemen in het gebruik en de ontwikkeling van artificiële intelligentie (AI). Hoewel deze technologie aanzienlijke kansen biedt om processen te optimaliseren, brengt zij ook belangrijke uitdagingen met zich mee op het vlak van controle, transparantie en verantwoordelijkheid.



Het onjuiste gebruik van AI-systemen heeft geleid tot diverse incidenten en controverses, wat de noodzaak aantoont om duidelijke kaders voor governance en naleving van regelgeving vast te stellen. In deze context moeten organisaties niet alleen het potentieel van AI begrijpen, maar ook de risico's die gepaard gaan met de implementatie ervan actief beheren.

Als advocaat en adviseur zie ik dit dagelijks: veel bedrijven gebruiken AI om tijd te besparen, maar vergeten dat zij geen gevoelige bedrijfsgegevens mogen invoeren. Daarnaast vergeten zij dat deze technologie fouten maakt en menselijke controle vereist.

Investeren in het gebruik en/of de implementatie van AI zonder de vertrouwelijkheid te beschermen en de betrouwbaarheid te garanderen, is als het bouwen van een luxueus gebouw op drijfzand. De bedrijfswaarde ligt niet alleen in het gebruik van de tool, maar ook in het beschermen van de informatie die eraan wordt toevertrouwd en het waarborgen van de juistheid ervan.

Daarom hebben wij deze white paper opgesteld. Hierin trachten wij de belangrijkste aspecten te bundelen waarmee AI-gebruikers rekening moeten houden. In deze white paper vindt u eveneens een lijst met "do's en don'ts". Beschouw dit als een praktische leidraad.

Laura Van Gompel, Managing partner

VGA
LAW & ADR

EEN EERSTE BLIK OP UW AI-COMPLIANCENIVEAU

Wetgevend kader:

- AI Act - Verordening (EU) 2024/1689
- Algemene Verordening Gegevensbescherming - Verordening (EU) 2016/679 (AVG)

Wat wordt beschouwd als een AI-systeem?

Volgens de AI-Verordening is een AI-systeem een op een machine gebaseerd systeem dat is ontworpen om met verschillende niveaus van autonomie te functioneren, dat na de implementatie een aanpassingsvermogen kan vertonen en dat, op basis van de gegevens die het ontvangt en expliciete of impliciete doelstellingen, in staat is af te leiden hoe een output kan worden gegenereerd, zoals voorspellingen, inhoud, aanbevelingen of beslissingen, die invloed kunnen hebben op fysieke of virtuele omgevingen.

Welke activiteiten?

De AI-regelgeving is van toepassing op zowel **ontwikkelaars, aanbieders en gebruikers van AI.**

Zij is **niet van toepassing** op privégebruik, niet-professioneel gebruik, wetenschappelijk onderzoek of nationale veiligheid.

Belangrijke aandachtspunten bij de evaluatie

- Alle betrokken actoren – gebruikers, aanbieders, ontwikkelaars en distributeurs van AI-systemen – moeten een volledige inventaris opmaken van de AI-systemen die binnen de organisatie worden gebruikt en deze classificeren volgens de risicocategorieën die in de regelgeving zijn vastgesteld.
- Afhankelijk van deze classificatie verschillen de toepasselijke verplichtingen, in het bijzonder voor AI-systemen met een hoog risico.
- AI-systemen die als een onaanvaardbaar risico worden beschouwd, zijn verboden. Hun ontwikkeling, commercialisering en gebruik moeten aldus worden stopgezet.
- Het is essentieel om de in de regelgeving opgenomen verboden praktijken te identificeren en de niet-naleving ervan te voorkomen.
- De GDPR (AVG) houdt rechtstreeks verband met het gebruik van AI-systemen. Beide regelgevingen moeten daarom in samenhang worden toegepast.

Risicoclassificatie van AI-systemen

- **Minimaal risico**

Voorbeelden: videogames die gebruikmaken van AI, spamfilters, enz.

- **Beperkt risico**

Voorbeelden: chatbots, virtuele assistenten, tekst- of beeldgeneratoren, enz.

- **Hoog risico**

Voorbeelden: AI-toepassingen voor werkgelegenheid en personeelsbeheer, AI-systemen die voor onderwijsinstellingen (bijvoorbeeld: toegang tot onderwijs, enz.)

- **Onaanvaardbaar risico**

Voorbeelden: manipulatie en misleiding, sociale scoring, emotieherkenning, enz.

Praktische aanbevelingen

- Beperk de toegang tot persoonsgegevens en AI-systemen.
- Leg afspraken met leveranciers en derden contractueel vast.
- Waarborg de kwaliteit en bescherming van gegevens.
- Zorg voor transparantie ten aanzien van gebruikers.
- Ontwikkel interne beleidsregels, opleidingen en procedures voor een verantwoord gebruik van AI.



RISICO-IDENTIFICATIE

De AI-verordening van de Europese Unie heeft tot doel de veiligheid, de gezondheid en de grondrechten van personen te beschermen tegen de risico's van het gebruik van artificiële intelligentie, door **een risicogebaseerde benadering te hanteren**. Zij legt geen uniforme verplichtingen op voor alle AI-systemen, maar voorziet in een gelaagd systeem waarbij **de verplichtingen afhangen van het risiconiveau** van elk systeem.

De verplichtingen die op uw onderneming van toepassing zijn, zullen bijgevolg afhangen van de mogelijke impact of schade die het gebruik van AI kan veroorzaken. Daarom is het essentieel om de gebruikte AI-systemen correct te identificeren en in de juiste risicocategorie onder te brengen.



Het is van essentieel belang om alle mogelijke manieren in kaart te brengen waarop een AI-systeem schade of nadelige gevolgen kan veroorzaken, zowel op technisch, juridisch, ethisch als maatschappelijk vlak. De AI-verordening onderscheidt onder meer de volgende risicocategorieën:

- **Risico's voor de gezondheid of fysieke veiligheid**, bijvoorbeeld fouten in een medisch systeem of in geautomatiseerde machines.
- **Risico's voor de grondrechten**, zoals het recht op gelijke behandeling, gegevensbescherming, vrijheid van meningsuiting of het recht op een eerlijk proces.
- **Ongerechtvaardigde vooroordelen (bias)** in gegevens of modellen die kunnen leiden tot discriminerende resultaten.
- **Gebrek aan transparantie of traceerbaarheid**, waardoor het moeilijk wordt te begrijpen waarom een bepaalde beslissing is genomen.
- **Cyberbeveiligingsrisico's**, die manipulatie van het systeem of ongeoorloofde toegang tot gevoelige gegevens mogelijk maken.
- **Prestatie- of betrouwbaarheidsproblemen**, zoals fouten, onnauwkeurigheden of onbetrouwbare resultaten onder reële gebruiksomstandigheden.

Aanbeveling:

Beperk de evaluatie niet tot een gecontroleerde omgeving. Het is essentieel om het gedrag van het AI-systeem onder reële gebruiksomstandigheden te analyseren en de daadwerkelijke impact ervan op personen en gegevens te beoordelen.

Enkele voorbeelden van AI-systemen per risicocategorie

PERSONEELSBEHEER

- **Werving, promotie en ontslag**: AI-systemen die gebruikt worden om cv's te screenen, kandidaten te selecteren of beslissingen te nemen over eventuele promoties of ontslagen, worden beschouwd als een hoogrisico AI-systeem. Reden: AI kan leiden tot vooroordelen (bias) en discriminatie.
- **Aanwezigheidscontrole:** Het gebruik van gezichtsherkenning voor toegangscontrole of beveiliging wordt beschouwd als hoogrisico-AI.

In beide gevallen betekent dit dat moet worden voldaan aan strikte transparantieverplichtingen (naast de reeds bestaande regelgeving inzake gegevensbescherming).





ONDERWIJS

- **Toegang tot onderwijs**: AI-systemen die personen toegang verleent of weigert tot onderwijsinstellingen, wordt beschouwd als hoog risico. Hetzelfde geldt voor AI-systemen die personen toewijst aan onderwijsinstellingen.
- **Evaluatie van studenten**: Het gebruik van AI-systemen door een onderwijsinstelling om academische prestaties te beoordelen of examens automatisch te corrigeren, brengt risico's met zich mee op het vlak van objectiviteit en gelijke behandeling.

Hoog risico AI-systemen moeten waarborgen bieden tegen vooringenomenheid (bias) en moeten menselijke controle mogelijk maken.

FINANCIËN

- Kredietbeoordeling: AI die wordt gebruikt om de kredietwaardigheid of kredietscore van natuurlijke personen te beoordelen, wordt beschouwd als hoogrisico-AI.

KLANTENSERVICE

- Gelet op de transparantieverplichting (beperkt risico) moeten AI-chatbots gebruikers informeren dat zij in interactie zijn met een AI-systeem (niet-menselijke interactie).

VGA
LAW & ADR



DO'S

- Betrek de IT- en cyberbeveiligingsafdeling bij de implementatie en configuratie van AI-tools.
- Gebruik uitsluitend de door de onderneming goedgekeurde AI-tools en behoud steeds menselijke controle over de resultaten.
- Controleer altijd de juistheid en betrouwbaarheid van door AI gegenereerde inhoud voordat deze extern wordt gebruikt.
- Beoordeel of het gebruikte AI-systeem onder specifieke verplichtingen van de AI-verordening (AI Act) kan vallen.

VERANTWOORD GEBRUIK

- Voor brainstorming.
- Teksten samenvatten, na voorafgaande verificatie van alle gegenereerde gegevens.
- Vertaling van documenten en zakelijke communicatie.
- Spellingscontrole en verbetering van stijl.
- Automatisering van repetitieve administratieve taken met een laag risico.

DONT'S



- Gebruik van openbare of niet-goedgekeurde AI-systemen.
- Het oordeel van een deskundige of professional vervangen door AI.
- Ervan uitgaan dat door AI gegenereerde informatie altijd correct of actueel is.
- Vertrouwelijke informatie, contracten, persoonsgegevens of bedrijfsgeheimen invoeren in open AI-platformen.
- De door AI gebruikte bronnen, referenties of gegevens niet controleren.



CHECKLIST

Vul deze vragenlijst in om een eerste inzicht te krijgen in de impact van het gebruik van AI binnen uw onderneming:

1. Gebruikt uw onderneming AI-systemen in klantgerichte processen?

☐ JA
☐ NEE

2. Neemt uw AI-systeem beslissingen die gevolgen kunnen hebben voor de rechten van personen (zoals kredietbeoordelingen, personeelswerving of medische diagnoses)?

☐ JA
☐ NEE

3. Beschikt uw onderneming over een strategie voor de opslag en bescherming van persoonsgegevens die worden verwerkt door AI-systemen?

☐ JA
☐ NEE

4. Werd uw AI-systeem getraind met grote datasets en weet u of deze vrij zijn van vooroordelen (bias) of discriminatie?

☐ JA
☐ NEE

5. Communiceert u op een transparante manier naar klanten wanneer u AI-systemen gebruikt die hun gedrag of beslissingen kunnen beïnvloeden (zoals chatbots of gepersonaliseerde aanbevelingssystemen)?

☐ JA
☐ NEE

6. Heeft uw onderneming reeds een risicoanalyse uitgevoerd om te bepalen in welke categorie uw AI-systemen vallen (minimaal, beperkt, hoog of onaanvaardbaar risico)?

☐ JA
☐ NEE

7. Heeft u eindgebruikers geïnformeerd over de implementatie en het correcte gebruik van de AI-tool(s)?

☐ JA
☐ NEE

8. Bent u zich bewust van de mogelijke sancties bij niet-naleving van de AI-verordening?

☐ JA
☐ NEE

9. Houdt uw onderneming een register bij van de AI-tools die worden gebruikt en volgt zij het gebruik ervan op?

☐ JA
☐ NEE

10. Heeft u een risicoanalyse van uw AI-model uitgevoerd? Beschikt u over een instrument om het gebruik van het model op te volgen?

☐ JA
☐ NEE

11. Heeft uw onderneming een basisopleiding over AI georganiseerd? Beschikt u over registraties of bewijsstukken van deze opleidingen?

☐ JA
☐ NEE

12. Maakt uw onderneming gebruik van AI-systemen die geautomatiseerde beslissingen nemen? Worden deze beslissingen onderworpen aan menselijke controle of beoordeling?

☐ JA
☐ NEE

Conclusie

Indien u op meerdere vragen "Nee" hebt geantwoord, is het mogelijk dat uw onderneming niet volledig voldoet aan de vereisten van de AI-verordening (AI Act). In dat geval is het aangewezen om passende maatregelen te nemen.

Heeft u twijfels over het nalevingsniveau van de AI-regelgeving binnen uw onderneming?

Wij bieden een AI-audit aan om de status van uw AI-systemen te evalueren en na te gaan of zij voldoen aan de vereisten van de AI Act.



U kunt steeds contact opnemen met ons kantoor voor juridisch advies omtrent andere AI vraagstukken. Ons team van experts staat klaar om u te begeleiden en te ondersteunen.

info@vga.law