

Checklist AI-gebruik

De AFM kijkt bij AI niet alleen naar of je het gebruikt, maar vooral naar hoe bewust, beheerst en uitlegbaar je dat doet. Onderstaande checklist helpt om na te gaan waar de toezichthouder op let en hoe je daaraan als adviseur of kantoor invulling kunt geven.

Hier let de AFM op	Dit kun je als adviseur of kantoor doen
Bestuurlijke verantwoordelijkheid	Leg vast wie verantwoordelijk is voor AI-beleid en toezicht. Bespreek AI-gebruik periodiek in directie- of managementoverleg en leg besluiten vast.
Inzicht in AI-gebruik binnen de organisatie	Maak een overzicht van de AI-tools die binnen het kantoor worden gebruikt, ook gratis of informeel gebruikte tools. Breng per toepassing in kaart waarvoor die wordt ingezet.
Proportioneel beleid en governance	Stel een beknopt AI-beleid op met afspraken over gebruik, risico's, controles en evaluatie. Zorg dat beleid en beheersing passen bij de omvang en aard van het AI-gebruik.
Gebruik van generatieve AI	Maak duidelijke afspraken over waarvoor tools als ChatGPT of Copilot wel en niet mogen worden gebruikt. Zorg dat output niet zonder menselijke controle richting klant of dossier gaat.
Transparantie richting klanten	Bepaal in welke gevallen je klanten informeert over het gebruik van AI. Maak duidelijk welke rol AI speelt en dat de professionele verantwoordelijkheid bij het kantoor blijft liggen.
Uitlegbaarheid van uitkomsten	Gebruik AI alleen voor toepassingen waarvan medewerkers de output kunnen beoordelen en toelichten. Leg vast hoe je uitkomsten controleert en hoe je omgaat met afwijkende resultaten.
Datakwaliteit en databronnen	Gebruik betrouwbare, actuele en relevante data. Maak afspraken over welke gegevens wel en niet in AI-tools mogen worden ingevoerd.
Privacy en vertrouwelijkheid	Voer niet zomaar persoonsgegevens of vertrouwelijke klantinformatie in publieke AI-tools in. Controleer voorwaarden van leveranciers, dataopslag en het gebruik van ingevoerde gegevens.

Beheersing van bias en ethische risico's	Laat AI-uitkomsten altijd door mensen beoordelen, zeker als die invloed hebben op klanten of risicobeoordelingen. Besteed in beleid en training aandacht aan vooroordelen en ongewenste uitkomsten.
AI-geletterdheid van medewerkers	Zorg dat medewerkers voldoende kennis hebben van de werking, kansen, beperkingen en risico's van AI. Stem instructie en training af op hun rol.
Uitbesteding en afhankelijkheid van leveranciers	Kijk kritisch naar aanbieders van AI-oplossingen en cloudproviders. Breng risico's als vendor lock-in, continuïteit en beveiliging in kaart en leg afspraken goed vast.
Menselijke controle op AI-gebruik	Zorg dat AI ondersteunend blijft en nooit het professionele oordeel vervangt. Leg vast bij welke processen menselijke controle altijd verplicht is.