

Tekst **Martijn Kortier**Martijn Kortier is advocaat Intellectuele eigendom,
ict-recht en privacy bij Elferink & Kortier Advocaten

Europese AI-Act

Met de Europese AI-Act, gepubliceerd op 12 juli 2024, verandert er veel voor gebruikers van AI-systemen. Wat zijn de belangrijkste privacyaspecten die gebruikers moeten kennen en waarom is naleving van zowel de AI-Act als de AVG cruciaal?

AI-systemen verwerken vaak grote hoeveelheden persoonsgegevens, zoals tekst, afbeeldingen en gedragsgegevens. Deze verwerking valt onder de Algemene verordening gegevensbescherming (AVG). Gebruikers van AI-systemen moeten dus ook voldoen aan de regels van de AVG.

Onder persoonsgegevens wordt verstaan alle informatie die betrekking heeft op een geïdentificeerde of identificeerbare. Dat varieert van namen tot complexe gegevens zoals IP-adressen, locatiegegevens en online identificatoren. AI-systemen kunnen persoonsgegevens direct (zoals namen) of indirect (zoals gedragsgegevens) verwerken. AI kan patronen herkennen die gevoelige details onthullen, zoals medische aandoeningen of politieke opvattingen. Hierdoor kunnen zelfs anonieme datasets in de context van AI als persoonsgegevens worden beschouwd, wat de toepassing van de AVG vergroot. Een kernprincipe van de AVG is transparantie. Gebruikers van AI-systemen moeten duidelijk communiceren over welke gegevens zij verzamelen, hoe deze worden gebruikt en met welk doel. Betrokkenen moeten geïnformeerd worden en soms toestemming geven voor de verwerking van hun gegevens met AI. Dit is vooral belangrijk bij gevoelige gegevens, zoals gezondheidsinformatie.

Transparantie betekent ook dat gebruikers van AI-systemen moeten kunnen uitleggen hoe en waarom een AI-systeem beslissingen neemt. Dit is een uitdaging door de *black box*-problematiek: AI-algoritmen, vooral die gebaseerd op *deep learning*, zijn vaak complex en ondoorzichtig. Hoe kun je transparant zijn als je de werking van de algoritmen zelf niet volledig begrijpt? Mogelijk moeten aanbieders van AI-systemen meer informatie geven over de werking van hun systemen.

Onder de AVG hebben betrokkenen rechten zoals inzage, correctie en verwijdering van hun gegevens. Gebruikers van AI-systemen moeten mechanismen implementeren om deze rechten te waarborgen. Als een individu vraagt om gegevens te verwijderen, moet het AI-systeem dit verzoek wel kunnen verwerken en de gegevens daadwerkelijk kunnen verwijderen. Dit kan een probleem worden als AI-systemen deze gegevens gebruiken om verder te leren.

De AVG vereist in sommige gevallen een Data Protection Impact Assessment (DPIA) voordat persoonsgegevens mogen worden verwerkt, vooral bij nieuwe technologieën als AI. Een DPIA is verplicht als de verwerking waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van personen. Gebruikers van AI moeten beoordelen of een DPIA vereist is. Het DPIA helpt bij het identificeren en minimaliseren van risico's van gegevensverwerking, wat essentieel is voor naleving van zowel de AVG als de AI-Act.

De advocaten en juristen van Elferink & Kortier Advocaten schrijven op deze plek iedere maand een column, waarin zij een praktisch probleem op het gebied van de AVG in relatie tot informatiebeheer behandelen. Heeft u een praktijkvraag die u behandeld wilt zien? Stuur deze naar Od@publiekdenken.nl.