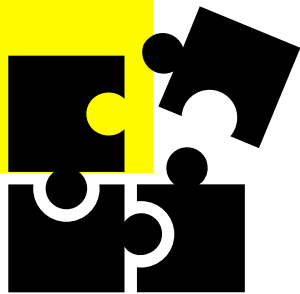


De juridische puzzel van AI Agents



Sdim – 9 juni

Susanna Nijsten & Isa Nieuwstad

The logo consists of the letters 'D', 'D', 'M', and 'A' stacked vertically. Each letter is stylized with a thick grey outline and a yellow fill. The 'D's are rounded, while the 'M' and 'A' have more angular, blocky shapes.

Visie

DDMA staat voor succesvolle en verantwoorde data-driven marketing. Marketing die mensen in beweging brengt, door data, technologie en creatie elkaar te laten versterken.

Verantwoord omgaan met data en technologie is daarbij essentieel. Voor het vertrouwen van consumenten én de toekomst van de marketingsector.

▶ Wat kan?

▶ Wat mag?

▶ Wat zou je moeten willen?



Susanna Nijsten
Legal Counsel
CAICO, CIPP/E

DDMA



Isa Nieuwstad
Legal Counsel
CIPP/E

DDMA

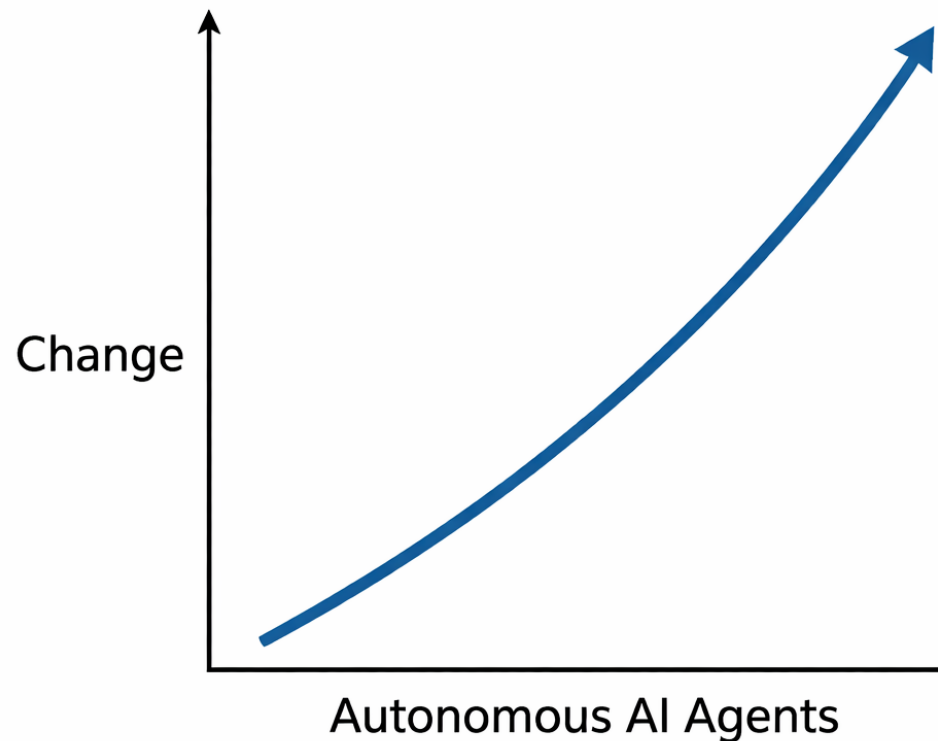
AI-generated







Internet of Agents?



- Agents/agentic AI binnen organisaties: beperkte impact op consumenten, maar wel: AVG/privacy en AI Act (zoals AI-geletterdheid).
- AI agents in contact met consumenten: bestaande regels voldoen, maar risico's nemen toe, minder menselijk toezicht vergroot kans op misleiding en fouten.
- Internet of Agents: consument en organisatie handelen via eigen agents, **regels verschuiven fundamenteel**.

Doel vandaag
Context, uitleg en inspireren ✨

AI Agents veranderen bestaande risico's

Normale risico's uitvergroot bij agents, bijv:

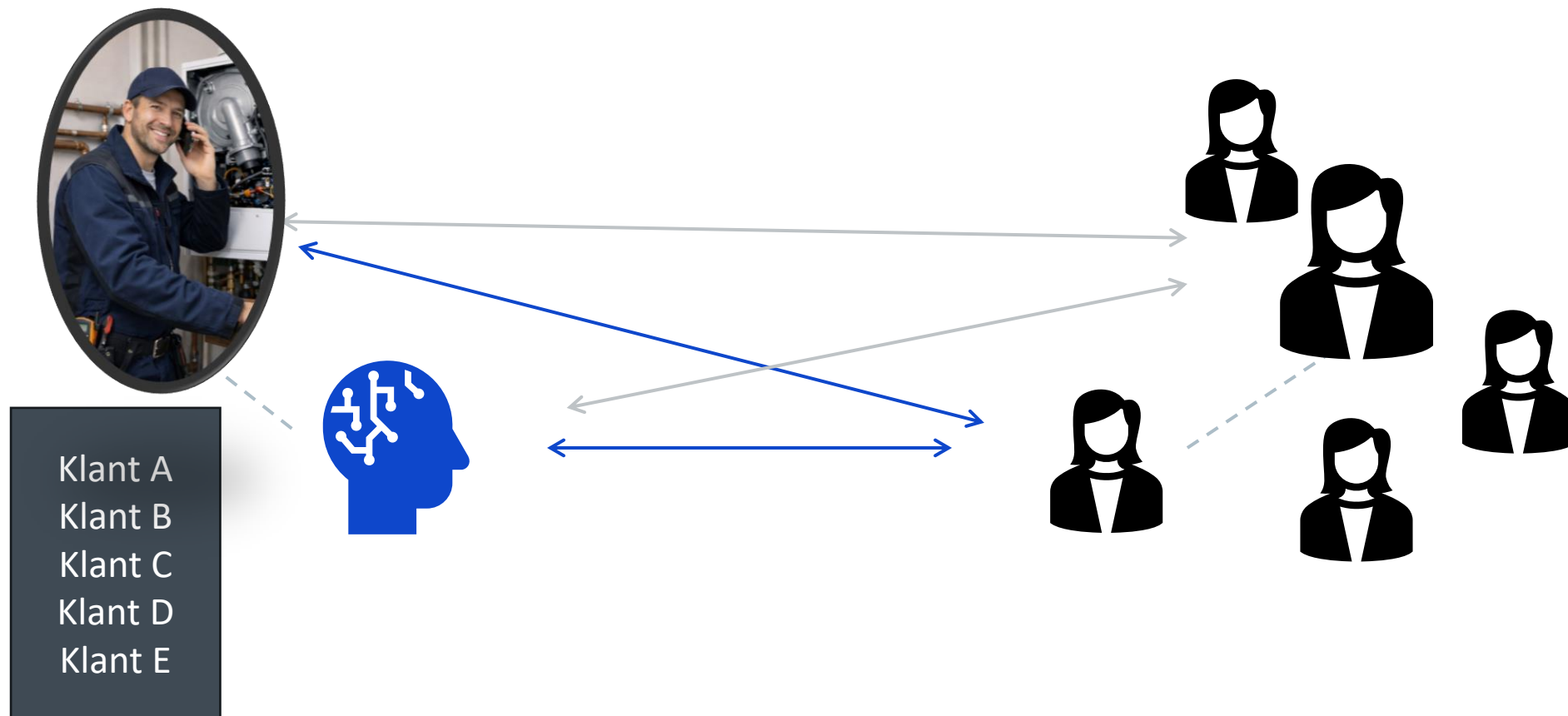
- Misinformatie
- Cyberveiligheid (botnet-gevaar, malafide agents)
- Authenticatie en privacy
- Hallucinaties
- Verlies overzicht, controle en transparantie: waar gaat info heen?

AI Agents veranderen recht

- ▶ Consument sluit overeenkomst met de AI Agent van je organisatie
- ▶ AI Agent komt contractuele afspraak niet na
- ▶ Persoonsgegevens worden gebruikt AI Agent te trainen
- ▶ AI Agent kan autonoom beslissingen maken buiten het menselijk toezicht

Hoe worden AI Agents gezien binnen huidige regels?

AVG



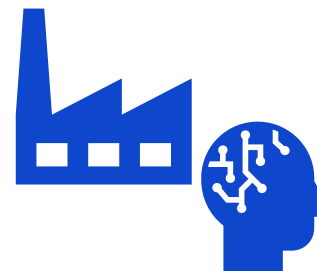
AVG-rollen

Verwerkingsverantwoordelijke

- Bepaalt doel en middelen van verwerking

Verwerker

- Handelt in opdracht van verantwoordelijke



Sluit een verwerkersovereenkomst!

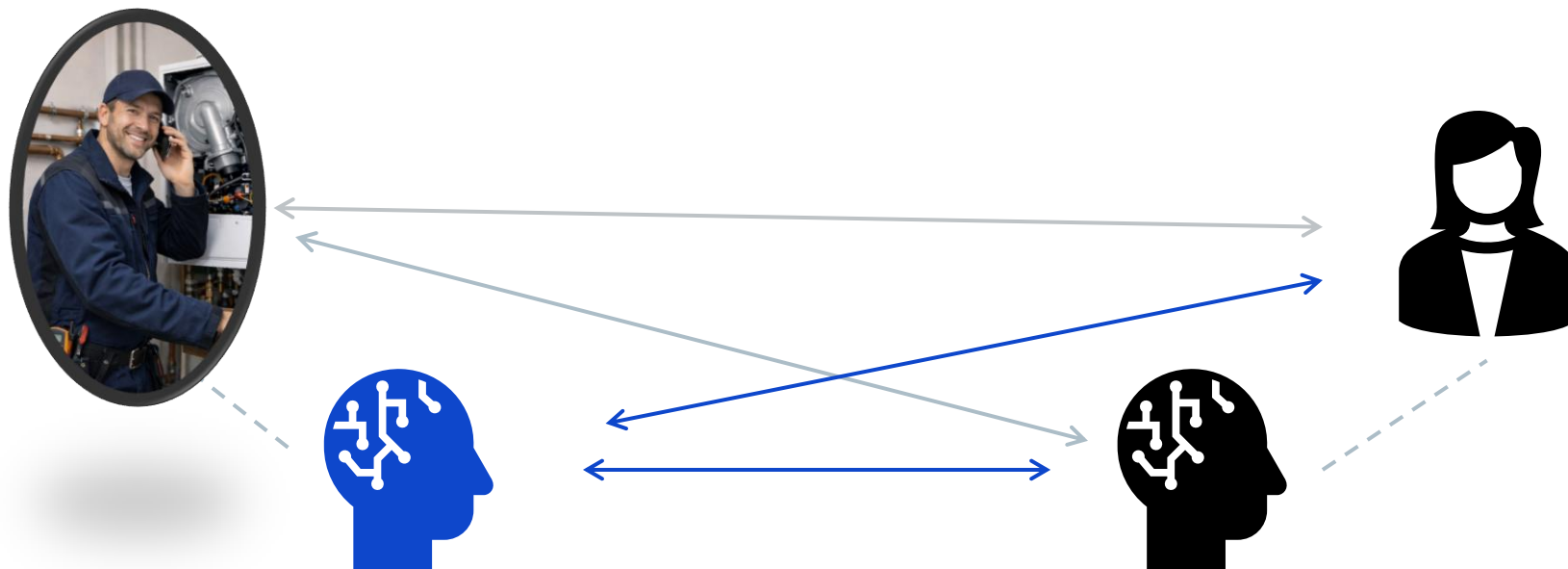
- Neem op:
 - Verbod gebruik persoonsgegevens eigen modeltraining
 - Afspraken loggen prompts, human in the loop momenten
 - Transparantie over subverwerkers (bijv. LLM-providers)
 - Uitsluitend handelt op gedocumenteerde instructies

Zet je AI Agents in? Denk dan na over het volgende:

- ▶ Begin met **AVG**-beginselen;
 - Rechtmatigheid (grondslag), doelbinding, dataminimalisatie, ...
- ▶ Doe een **DPIA**;
- ▶ Ben transparant richting betrokkenen;
- ▶ Juiste waarborg internationale doorgifte;

Contracten en aansprakelijk- heid

Contracten?



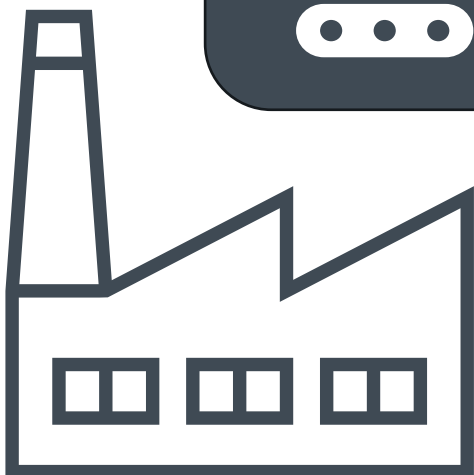
Guiding Principles and Model Rules on Digital Assistants for Consumer Contracts

European Law Institute

Wat is belangrijk?

- ▮ Gebruik AI Agent geen invloed op **geldigheid** contract
- ▮ **Consumentenrecht** is van toepassing bij handel met consument, ongeacht gebruik AI Agent
 - ▮ Organisatie mag consument **niet** verbieden óf verplichten AI Agent te gebruiken
- ▮ Informatieplicht = 'human-readable' én 'machine-readable'
 - ▮ Zo kan AI Agent ook een samenvatting aan consument geven
- ▮ **Communiceer** over gebruik AI Agent
 - ▮ **Technisch** of op een andere duidelijke en begrijpelijke wijze
 - ▮ Niet gedaan? Reden voor consument om geen contract te willen? Contract beëindigen

Wie is aansprakelijk?



Verkeerde antwoorden

Getraind op juiste data



**Afspraken maken voor
cosmetische ingrepen**

**AI chatbot: verkeerde
medische titel**

Is AI chatbot een derde partij of bedrijf aansprakelijk?

Uitspraken DUI en CAN

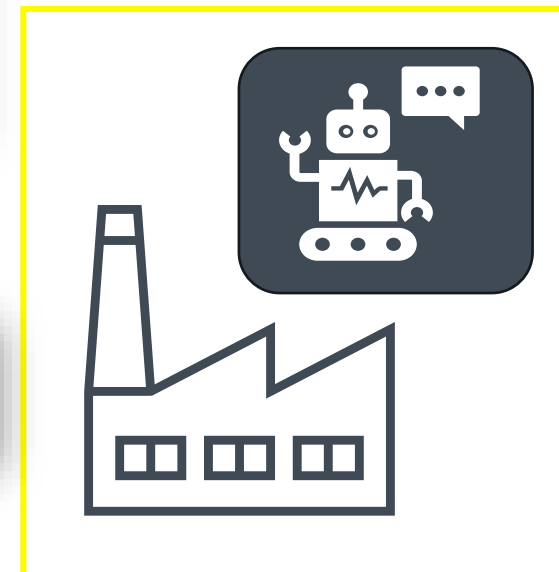
Higher Regional Court of Hamm: Judgment in the case of the Consumer Center of North Rhine-Westphalia against Aesthetify GmbH

May 12, 2026



Air Canada moet klant vergoeden na misleiding door chatbot

maandag 19 februari 2024, 12:04 door [Redactie](#), 13 [reacties](#)



Verantwoordelijkheid

- ▶ Degene die AI Agent gebruikt is gebonden aan de acties die worden genomen door de AI Agent
 - Verantwoordelijkheid gebruiker
- ▶ Uitsluiting van aansprakelijkheid voor AI Agent in contract?
 - → Niet mogelijk





AI Act

AI Agents en de AI Act

- Definieert als zowel AI-systeem als GPAI-model
- AI-systeem:
 - Verbod: schadelijke manipulatie en uitbuiting kwetsbaarheden
 - Transparantie nodig wanneer het de bedoeling is dat agent contact heeft met personen óf content genereert
 - Chatbots voor klantcontact, coding agents, plant meetings, maakt social posts, beheert ad campaigns
- GPAI-models
 - Afhankelijk level van autonomie of Agent een beperkt risico heeft
 - Risico management verplichtingen

Typically, an AI agent will contain at least a general-purpose AI (GPAI) model, and constitute an AI system as it will usually have some form of interface, which is considered a system component (recital 97 AI Act). A more precise statement than 'typically' is difficult to make as the term AI agent is not legally defined and is used colloquially for different kinds of artefacts. Thus, while AI agents are not a separate category of AI under the AI Act, the definitions of an AI system in Article 3(1) AI Act and of a GPAI model in Article 3(63) AI Act are sufficient to cover AI agents. This means that the rules applicable to AI systems and GPAI models under the AI Act also apply to AI agents.

AI-geletterdheid



Verplicht voor aanbieders, gebruikers en namens hen...



Geen specifieke vereisten per sector



Geen test / certificaat nodig



Doelgroepgerichte training



Risicogebaseerde aanpak vereist



Handleiding niet voldoende



Brede kennis vereist (ook ethisch en juridisch)



Geen verplichte AI-officer



Geen vereisten voor 'voldoende' AI-geletterdheid



Vorbereiden op handhaving

Transparantie- verplichtingen AI

Transparantie en AI

- ▶ Transparantie bij AI-agents
- ▶ Transparantie bij content creatie
- ▶ Transparantie verplichtingen AI Act
 - 2 augustus > 2 december 2026

Transparantie- verplichtingen AI agents

Transparantie bij AI-agents

AI Act

- Direct contact met een natuurlijk persoon
 - Hoeft niet door de natuurlijke persoon te worden geïnitieerd
- Voorbeelden
 - Wel: AI-enabled voice assistant, chatbots en conversational agents, AI companions en andere agentic AI-systemen
 - Niet: geautomatiseerde vertalingen of transcriptietools, systemen waar de gebruiker alleen de output van de AI ziet zonder te kunnen reageren hierop

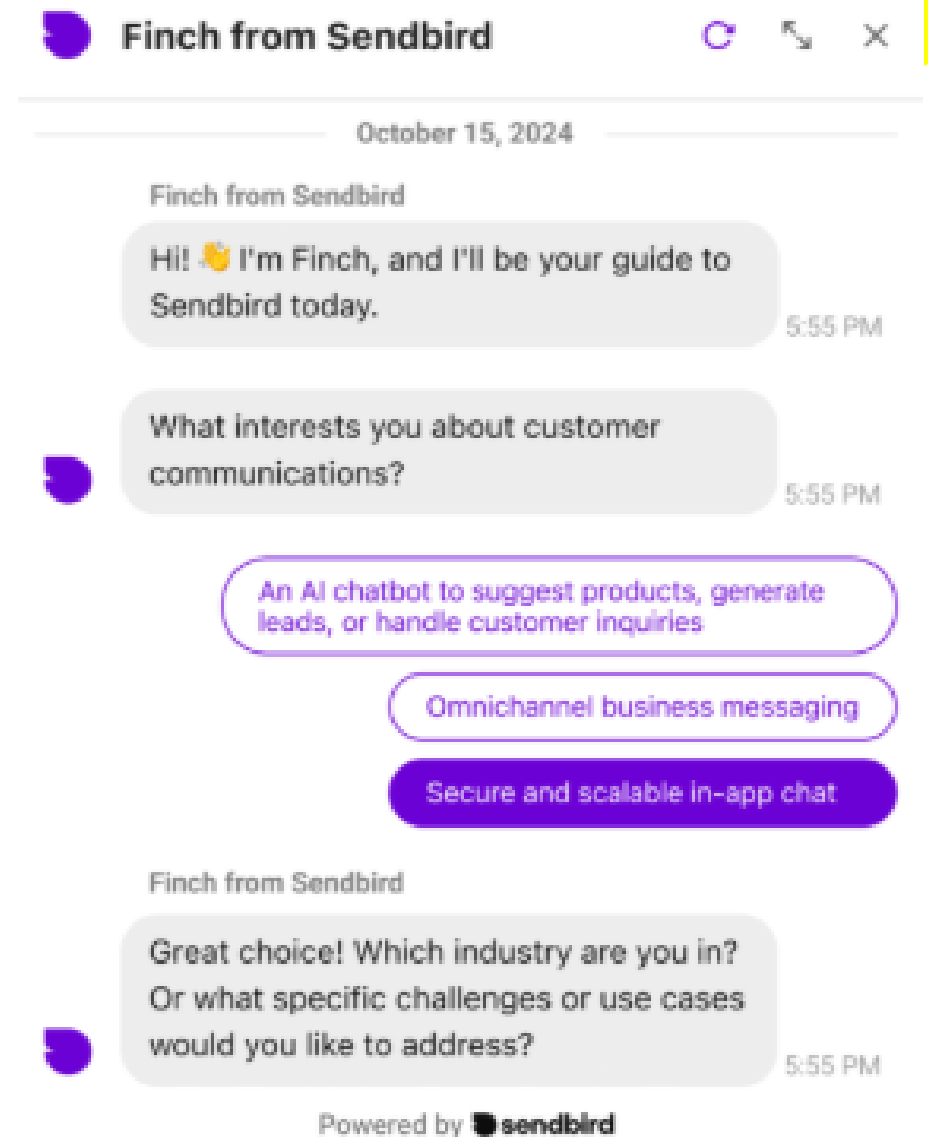


Transparantie bij AI-agents

AI Act

Hoe doe je dat dan?

- Eerste moment van interactie
- Informatie is duidelijk en te onderscheiden
 - Geen specifieke techniek vereist
 - Advies is aansluiten bij gebruikte modaliteit of zelfs multi-modaal
 - Alleen in URL of documentatie is niet voldoende
 - 'Human-readable'
- Je houdt rekening met je doelgroep en hun kennisniveau
 - Ouderen vs. developers



- Uitzondering: een label is niet nodig wanneer het overduidelijk AI is
- Dit hangt af van:
 - Hoe overduidelijk AI de interactie is én
 - Wat de doelgroep en hun kennisniveau is
- Overduidelijk = goed geïnformeerde en oplettende gebruiker uit de doelgroep
- Doelgroep = mensen die redelijkerwijs met het AI-systeem in aanraking kunnen komen

**Transparantie-
verplichtingen
AI content
creatie**

Twee verschillende regimes:

- 'Gewone' AI-gegenereerde content
- Deepfakes en teksten voor algemeen belang



'Gewone' AI-gegenereerde content

AI Act

- Je gebruikt een algemeen beschikbare GenAI om content te creëren
 - Blog of rapport schrijven
 - Afbeelding of video creëren
- Transparantieregels gelden voor de aanbieder
 - Degene die de AI heeft ontwikkeld of laten ontwikkelen
 - En onder eigen naam op de markt brengt
- Technische markering
- Uitzondering: standaard editing en minimale aanpassingen



- ▶ Deepfakes
 - Teksten van algemeen belang
 - Transparantieregels gelden voor de gebruiksverantwoordelijke
 - Degene die de AI onder eigen verantwoordelijkheid gebruikt in het kader van een beroepsactiviteit

- Publiek informeren over aangelegenheden van maatschappelijk belang
 - Gepubliceerde tekst = public access
 - Publiek informeren = doel van de tekst is kennis, meningen of feiten overbrengen
 - Maatschappelijk belang = onderwerpen die belangrijk zijn voor de maatschappij, deze onderwerpen kunnen door de tijd heen veranderen
- Uitzondering: wanneer de tekst is nagekeken door een mens én een (rechts)persoon de redactionele verantwoordelijkheid op zich neemt

- ▼ Wanneer is er sprake van een deepfake?
 - Beeld-, audio- of videomateriaal
 - Gelijkenis bestaande personen, plaatsen, entiteiten of gebeurtenissen
 - Personen: bestaand of zou kunnen hebben bestaan
 - Ten onrechte als authentiek gezien kan worden
 - Intentie van de maker maakt niet uit
- Uitzondering: artistieke en satirische werken
 - Wel een label, maar minder prominent
 - Advertenties en commerciële uitingen vallen hier niet onder



Transparantie bij AI content creatie

AI Act

- AI-presentatrice Kids Top20
- YouTube-kanaal klusjesman
 - Realistische AI-gegenereerde influencer
 - Cartoon hamer en boor



Deepfake & teksten van algemeen belang

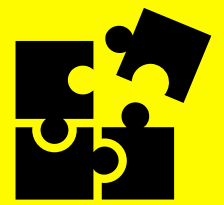
- ▶ Hoe doe je dat dan?
 - Duidelijk zichtbaar AI-label
 - Aanpassen aan context en modaliteit
 - 'Human-readable'
 - Eerste moment van interactie

AI Act



- AI Act specifieke transparantieverplichtingen AI-aard systeem
- Andere wetgeving:
 - Oneerlijke handelspraktijken
 - Consumentenrecht
 - AVG
- Uitgangspunt: consument mag niet misleid worden en moet een geïnformeerde keuze kunnen maken

5 tips oplossen van AI Agent puzzel



- Denk in kansen, beperk risico's
 - Human in the loop
- **Begin bij de basis:** zorg voor voldoende (juridische) kennis
- Ben transparant over gebruik AI Agent
- Zorg voor een goede **AI-governance**;
 - AI Beleid, AI Impact Assessments, AI Taskforce
- Blijf op de hoogte van de laatste ontwikkelingen...

Vragen?

legal@ddma.nl



Susanna Nijsten
Legal Counsel
DDMA



Isa Nieuwstad
Legal Counsel
DDMA



Sara Mosch
Senior Legal Counsel
DDMA