

LES 04

# AI & de wet

Juridische kaders, auteursrecht en aansprakelijkheid in bibliotheekcontext

 90 min | Alle bibliotheekprofessionals

# Het juridische landschap

implementatie in bibliotheken roept dringende juridische vragen op in vier onderling verbonden domeinen:

## © Auteursrecht

Wie bezit AI-output? Wat zijn de risico's rond trainingsdata en AI-ondersteunde contentcreatie?

## EU AI Act

De eerste AI-wet ter wereld, met risicoclassificatie, verplichtingen voor gebruiksverantwoordelijken en handhaving.

## Gegevensbescherming

Hoe is de GDPR/AVG van toepassing wanneer AI gegevens van bezoekers, vragen of gebruikersprofielen verwerkt?

## Aansprakelijkheid

Wat gebeurt er wanneer AI fouten maakt? Wie is verantwoordelijk: de bibliotheek of de leverancier?

# Auteursrecht en AI

## TRAININGSDATA

AI-modellen worden getraind op enorme datasets die vaak auteursrechtelijk beschermd materiaal bevatten. Drie belangrijke juridische vragen voor bibliotheken:

- 1 Hebben AI-ontwikkelaars toestemming nodig om auteursrechtelijk beschermde content te gebruiken voor training?
- 2 Vormt training op auteursrechtelijk beschermd materiaal een inbreuk op het auteursrecht?
- 3 Hoe verschillen de EU, de VS en het VK in hun uitzonderingen voor tekst- en datamining (TDM)?

### EU Copyright Directive (2019/790)

Introduceerde een uitzondering voor tekst- en datamining voor onderzoeksorganisaties en instellingen voor cultureel erfgoed. Bibliotheken kunnen daarvoor in aanmerking komen, maar of dit ook geldt voor commerciële AI-training blijft betwist.

# Auteursrecht en AI

## WIE BEZIT AI-GEGENEREERDE OUTPUT?

### De meeste rechtsgebieden

Auteursrecht vereist menselijk auteurschap. AI-gegenereerde content zonder betekenisvolle menselijke creatieve inbreng is mogelijk niet auteursrechtelijk beschermd.

### Leveranciersvoorwaarden variëren

Gebruiksvoorwaarden lopen sterk uiteen. Output kan toebehoren aan de gebruiker, aan de leverancier of volledig in het publieke domein vallen.

### Praktische implicatie voor bibliotheken

Controleer leverancierscontracten zorgvuldig om te begrijpen wie eigenaar is van AI-gegenereerde content, vooral wanneer die content gepubliceerd of extern gedeeld wordt, zoals catalogusrecords, zoekhulp of publieksgerichte teksten.

# Gegevensbescherming en AVG

Wanneer AI-systemen persoonsgegevens verwerken, zoals vragen van bezoekers, uitleengegevens of onderzoeksprofielen, is GDPR/AVG van toepassing.

## Rechtsgrond

Bibliotheken moeten een geldige rechtsgrond bepalen voor de verwerking van persoonsgegevens met AI, zoals gerechtvaardigd belang, toestemming of publieke taak.

## Dataminimalisatie

AI-tools mogen niet meer persoonsgegevens verzamelen of verwerken dan noodzakelijk is voor het opgegeven doel.

## Geautomatiseerde beslissingen

Artikel 22 GDPR/AVG beperkt volledig geautomatiseerde beslissingen met significante gevolgen, waaronder AI-gebaseerde profilering en toegangssystemen.

## DPIA's vereist

Gegevensbeschermingseffectbeoordelingen (DPIA's) zijn verplicht wanneer de verwerking waarschijnlijk een hoog risico oplevert. AI-tools die gebruikers profileren, vallen daar vrijwel zeker onder.



Bibliotheek = verwerkingsverantwoordelijke. AI-leverancier = verwerker. Een AVG-conforme verwerkingsovereenkomst (DPA) is verplicht.

WAAROM DE EU AI ACT?



# De EU AI Act



## Dutch Rutte government resigns over child welfare fraud scandal



Dutch PM Mark Rutte said in January 2021 the decision to resign was "unavoidable"



You're a single mother with three children aged eight to 11. You hit rock-bottom financially and think what now? My children and I sometimes had to go to bed without food

**Dulce Gonçalves Tavares**

Told in 2013 she had to pay back €125,000



Last month, Prime Minister of the Netherlands Mark Rutte—along with his entire cabinet—resigned after a year and a half of investigations revealed that since 2013, 26,000 innocent families were wrongly accused of social benefits fraud partially due to a discriminatory algorithm.



## **Audit of 9 government algorithms finds 6 do not meet basic requirements**

News item | 18-05-2022 | 10:45

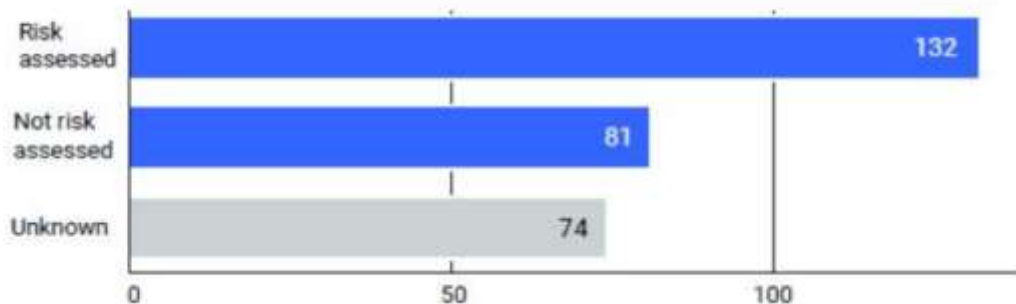
Responsible use of algorithms by government agencies is possible but not always the case in practice. The Netherlands Court of Audit found that 3 out of 9 algorithms it audited met all the basic requirements, the other 6 did not and exposed the government to various risks: from inadequate control over the algorithm's performance and impact to bias, data leaks and unauthorised access.

# De EU AI Act



**Figure 14** *Risk assessment of AI systems*

Not all AI systems underwent a risk assessment



This figure presents information on only the 287 AI systems currently under development or in use.



# De EU AI Act

Het eerste omvattende juridische kader ter wereld voor artificiële intelligentie: risicogebaseerd, bindend en van kracht.

**ONAAANVAARDBAAR RISICO** — Verboden praktijken. Volledig verboden.

**HOOG RISICO** — Strikte eisen, menselijk toezicht en impactbeoordelingen verplicht.

**BEPERKT RISICO** — Transparantieverplichtingen; maak AI-gebruik kenbaar aan gebruikers.

**MINIMAAL RISICO** — Geen specifieke verplichtingen; vrijwillige gedragscodes worden aangemoedigd.



# De EU AI Act

## Onaanvaardbaar risico

- Subliminale, misleidende of manipulatieve technieken
- Uitbuiting van persoonlijke kwetsbaarheden
- Biometrische categoriseringssystemen die gevoelige kenmerken afleiden
- Een sociale score toekennen
- Het inschatten van het risico dat een individu strafbare feiten zal plegen
- Databanken voor gezichtsherkenning samenstellen
- Emoties afleiden in werkomgevingen of onderwijsinstellingen
- Realtime biometrische identificatie op afstand in publiek toegankelijke ruimten voor rechtshandhaving



# De EU AI Act

## Hoog risico

- Niet-verboden biometrie
- Kritieke infrastructuur
- Onderwijs en beroepsopleiding
- Werkgelegenheid, personeelsbeheer en toegang tot zelfstandige arbeid
- Toegang tot en gebruik van essentiële publieke en private diensten
- Rechtshandhaving
- Migratie-, asiel- en grenscontrolebeheer
- Rechtsbedeling en democratische processen



# De EU AI Act

## Hoog risico

Leveranciers moeten onder meer aan deze eisen voldoen:

- Risicobeheersysteem
- Datagovernance
- Technische documentatie
- Logboekregistratie
- Gebruiksaanwijzing
- Mogelijkheid tot menselijk toezicht



# De EU AI Act

## Beperkt risico

- Verplichte transparantie
- *Voorbeelden: deepfakes*

## Minimaal risico

- Niet gereguleerd
- *Voorbeelden: spamfilters en AI-videogames*

# De EU AI Act – gebruikscases voor bibliotheken

Waar vallen AI-tools in bibliotheken binnen de risicoclassificatie?

| Casus                                                  | Risiconiveau                                                                                                   | Verplichting                                          |
|--------------------------------------------------------|----------------------------------------------------------------------------------------------------------------|-------------------------------------------------------|
| Sociale scoring / surveillance van bezoekers           |  <b>Onaanvaardbaar risico</b> | Verboden; nooit inzetten                              |
| Profilering van bezoekers / voorspelling van gedrag    |  <b>Hoog risico</b>           | Menselijk toezicht en incidentlogging verplicht       |
| AI-chatbot voor referentievragen                       |  <b>Beperkt risico</b>        | Gebruikers moeten weten dat ze met AI communiceren    |
| AI-gegenereerde contenttools                           |  <b>Beperkt risico</b>        | Output duidelijk labelen als AI-gegenereerd           |
| AI-ondersteunde catalografie als tool voor medewerkers |  <b>Laag risico</b>           | Geen specifieke verplichtingen, volg goede praktijken |

# EU AI Act - verplichtingen voor bibliotheken als gebruiksverantwoordelijken

Bibliotheken die AI-tools gebruiken, zelfs als eindgebruikers, zijn volgens de AI Act gebruiksverantwoordelijken en hebben wettelijke verplichtingen.

## HOOG-RISICOSYSTEMEN

- Voer vóór inzet een grondrechten-effectbeoordeling uit
- Houd logs bij en zorg altijd voor menselijk toezicht
- Informeer personen wanneer zij onderworpen zijn aan AI-ondersteunde beslissingen.

## ALGEMENE AI-TOOLS (vb. LLM's als ChatGPT, Claude, Gemini)

- Gebruik de tools alleen binnen het doel dat de leverancier heeft bepaald
- Zet ze niet in op manieren die risico's creëren die niet in de documentatie zijn opgenomen
- Vraag conformiteitsdocumentatie aan leveranciers vóór je tekent

## AI-GEGENEREERDE CONTENT EN CHATBOTS

- Maak aan gebruikers duidelijk dat zij met een AI-systeem communiceren
- Label alle AI-gegenereerde output duidelijk en consequent
- Gebruik geen deepfakes of synthetische media zonder duidelijke bekendmaking

# Aansprakelijkheid - wanneer AI in de fout gaat

AI-systemen kunnen onjuiste, bevooroordeelde of schadelijke output produceren. In bibliotheekcontext kan dat gaan om :

## Onjuiste records

Onjuiste bibliografische records of citaties die door AI-catalogafietools worden gegenereerd.

## Bevooroordeelde output

Discriminerende of bevooroordeelde output in AI-gestuurde aanbevelings- of toegangssystemen.

## Privacyschendingen

Privacyschendingen door AI-gegenereerde content die naar echte personen verwijst.

## Desinformatie

Desinformatie die via AI-gestuurde referentie- of vraag-en-antwoordtools wordt gepresenteerd.

Leverancierscontracten zijn je eerste verdedigingslinie. Zorg dat ze bepalingen bevatten over vrijwaring, aansprakelijkheidsplafonds, garanties rond juistheid, melding van incidenten en overdraagbaarheid van gegevens bij beëindiging.

# De juridische blik van de bibliothecaris

De vaardigheden die je al gebruikt om bronnen te evalueren, zijn rechtstreeks toepasbaar op AI-recht.

| Rechtsgebied         | Belangrijkste vraag                                                                                    |
|----------------------|--------------------------------------------------------------------------------------------------------|
| Auteursrecht         | Wie bezit output van deze tool en is de tool getraind op auteursrechtelijk beschermd materiaal?        |
| Gegevensbescherming  | Verwerkt deze tool persoonsgegevens? Is een DPIA en verwerkingsovereenkomst vereist?                   |
| EU AI Act            | In welke risicocategorie valt dit systeem? Wat zijn onze verplichtingen als gebruiksverantwoordelijke? |
| Aansprakelijkheid    | Als deze AI een fout maakt of schade veroorzaakt, wie draagt dan de juridische verantwoordelijkheid?   |
| Leverancierscontract | Bevat het contract bepalingen over vrijwaring, melding van incidenten en rechten rond data-exit?       |

# Kernwoordenschat AI en recht

## EU AI Act

Verordening (EU) 2024/1689, de eerste omvattende AI-wet ter wereld, met een risicogebaseerde aanpak voor het reguleren van AI-systemen en hun gebruiksverantwoordelijken.

## GPAI-model

AI-model voor algemene toepassingen, bijvoorbeeld een LLM zoals GPT of Claude, gebruikt als fundament van een product. Onderworpen aan specifieke transparantieverplichtingen.

## Tekst- en datamining

Een auteursrechtelijke uitzondering die geautomatiseerde analyse van content toelaat, met verschillende voorwaarden in de EU, de VS en het VK.

## Gebruiksverantwoordelijke

Een organisatie, zoals een bibliotheek, die een AI-systeem gebruikt in haar werking. Dit is iets anders dan de aanbieder of ontwikkelaar van dat systeem.

## DPIA

Data Protection Impact Assessment of gegevensbeschermings-effectbeoordeling. Een door de GDPR/AVG vereiste procedure vóór de inzet van AI die waarschijnlijk een hoog risico inhoudt,.

## Vrijwaring

Een contractuele clausule waarbij één partij ermee instemt de juridische aansprakelijkheid of financiële verliezen van een andere partij te dekken.

# Groepsactiviteit – Regelgeving-challenge

- **Casus 1:** een bibliotheek gebruikt een AI-chatbot om boeken aan te bevelen. De chatbot slaat per ongeluk chatgeschiedenissen van bezoekers op, inclusief persoonlijke voorkeuren.
- **Casus 2:** een systeem voor gezichtsherkenning wordt voorgesteld voor beveiliging. Laat de AI Act dit toe? Welke waarborgen zijn nodig?
- **Casus 3:** een student genereert een essay met ChatGPT. De bibliotheek wordt gevraagd om de zoekgeschiedenis van de student met de school te delen.

Analyseer in je groep jullie casus over AI, gegevensprivacy en juridische naleving om te bepalen wat de beste aanpak is onder de regels van GDPR/AVG en de AI Act.



# Discussie

- 1 Heeft je instelling een aankoopbeleid voor AI? Wie controleert leverancierscontracten op juridische naleving?
- 2 Heb je AI-tools gebruikt om content te genereren, zoals records, samenvattingen of beschrijvingen? Wie bezit die content?
- 3 Hoe zou je de risicoclassificatie van de EU AI Act uitleggen aan een collega die er nog nooit van gehoord heeft?
- 4 Welke juridische vraag over AI in je bibliotheek voelt nu het meest dringend?