ICTRECHT

Cheat sheet

AI Act

Alles over de nieuwe regels voor AI en algoritmes.

Lees verder

Scope

01 Definitie van AI

AI-systemen die voor impliciete en expliciete doeleinden, met enige vorm van autonomie, zelf afleiden welke output te generen.*

*De AI Act bevat aparte regels voor AI-modellen voor algemene doeleinden.

02 Territorium

Aanbieders op de markt in de EU (ongeacht de vestigingsplaats), afnemers, importeurs, distributeurs, en gemachtigde vertegenwoordigers (van aanbieders).

03 Wie

Producenten, verkopers, distributeurs en afnemers.

04 Uitzonderingen

O.a. privégebruik in huiselijke sfeer, militaire toepassingen en nationale veiligheid, opsporing en handhaving (gedeeltelijk), wetenschappelijk onderzoek, en open source (zeer beperkt).

Risiconiveaus

01 Onacceptabel risico (verboden)

Manipulatieve technieken, misbruik maken van kwetsbaarheden, social scoring, emotieherkenning op werk, databanken voor gezichtsherkenning, real time biometrische identificatie op afstand (voor rechtshandhaving).

02 Hoog risico

Op basis van harmonisatiewetgeving in Bijlage I van de AI Act:

(Veiligheidscomponenten van) gereguleerde producten zoals medische hulpmiddelen, machines, motorvoertuigen, liften, speelgoed, etc.

Op basis van use cases in Bijlage III van de AI Act:

Biometrie, kritieke infrastructuur, onderwijs en beroepsopleiding, werkgelegenheid, essentiële diensten en uitkeringen, rechtshandhaving, rechtspraak, en migratie-, asiel- en grensbeheer. Tenzij het AI-systeem:

- Alleen menselijk werk verbetert.
- Alleen een beperkte procedurele taak uitvoert.
- Niet van invloed is op de beslissingen.
- Alleen voorbereidend werk doet.

03 Transparantierisico (‘laag risico’)

AI-systemen met directe interactie (o.a. chatbots), generatieve AI (tekst, beeld, audio, etc.), emotie-herkenning en biometrie (voor zover is toegestaan).

04 Restcategorie (‘minimaal of geen risico’)

AI-systemen die niet in de overige risicocategorieën vallen.

Compliance: Hoog risico

Documentatie

Duidelijke en concrete technische documentatie en gebruikshandleidingen.

Systeem voor risicomanagement en kwaliteitsbeheer

Potentiële risico's identificeren, evalueren, beheren en verminderen. Waarborgen van de kwaliteit.

Fundamental Rights Impact Assessment (FRIA)

Een gestructureerde analyse van de risico's voor fundamentele rechten uitvoeren.

Post market monitoring

Een systeem opzetten, dat gegevens over de prestaties van het AI-systeem gedurende de gehele levensduur verzamelt en analyseert.

Transparantie

Uitlegbaarheid, automatisch loggen en bewaren.

Conformiteitsbeoordeling

CE-markering aanbrengen zodra volledig aan AI Act is voldaan.

Menselijk toezicht

Mens betrokken in het proces (in-the-loop) of nauw toezicht (in command).

Accuraatheid, robuustheid en cyberbeveiliging

Risico's op bias output verkleinen, bestand zijn tegen fouten en storingen, en beveiliging tegen (cyber)dreigingen en misbruik.

Gegevensbeheer

Beheersen van representativiteit, kwaliteit en rechtmatigheid van data.

AI met transparantierisico's:

- Mensen informeren dat ze direct interacteren met een AI.
- Output van generatieve AI labelen.
- Informeren over biometrie en emotieherkenning (indien toegestaan).

AI-modellen voor algemene doeleinden:

- Beschikbaar stellen van technische documentatie en samenvattingen van trainingsdata.
- Beleid opstellen voor de naleving van auteursrechten. Voldoen aan praktijkcodes.
- Grote AI-modellen met 'systeemrisico' moeten aanvullende evaluaties en waarborgen realiseren.

Boetes en handhaving

Elke lidstaat krijgt minstens één toezichthouder. In Nederland zullen de huidige markttoezicht-houders en inspectiediensten toezicht houden op AI.

Toezichthouders mogen:

- Toegang eisen tot alle documentatie, broncode en model parameters.
- Bindende aanwijzingen geven over aangepast gebruik.
- Bevel tot staking geven indien de AI toch te risicovol blijkt.
- Boetes opleggen.

Vanaf wanneer?

12 juni 2024

Publicatie in Official Journal.

1 augustus 2024

AI Act in werking getreden. Regels worden gefaseerd van kracht.

2 februari 2025

- Verbod op onacceptabele AI.
- Verplichtingen AI-geletterdheid van kracht.

2 mei 2025

Deadline publicatie codes of practice (praktijk codes) voor AI-modellen voor algemene doeleinden.

2 augustus 2025

Regels van kracht met betrekking tot:

- AI-modellen voor algemene doeleinden.
- Conformiteitsbeoordelingsinstanties.
- Boetes.
- Deadline publicatie boeterichtsnoeren.
- Deadline oprichten toezichthouders (en implementatie van procedures).

2 augustus 2026

- Volledig van kracht voor alle vormen van AI (behalve Bijlage I) en bepaalde legacy IT-systemen).
- Deadline publicatie richtsnoeren voor post market monitoring.

2 augustus 2027

Regels voor hoog risico AI-systemen op basis van Bijlage I van kracht.

1 januari 2030

AI Act van toepassing op bepaalde grootschalige IT-systemen van de overheid (Bijlage X AI Act).

Boetes kunnen oplopen tot

EUR 35 miljoen

of bij bedrijven 7% van wereldwijde concernomzet bij inzet van verboden AI.

EUR 15 miljoen

of bij bedrijven 3% van wereldwijde concernomzet bij andere overtredingen.

EUR 7,5 miljoen

of bij bedrijven 1,5% van wereldwijde concernomzet bij verstrekken van onjuist, onvolledige of misleidende informatie aan toezichthouders.

Voor mkb en startups zullen lagere plafonds gaan gelden.

ICTRECHT

Wil je meer weten over de AI ACT?

Bezoek onze website voor het laatste nieuws, onze diensten en trainingen.

Vragen?

- www.ictrecht.nl/ai-act
- 020 - 663 1941