Embed AI

ANNEX III PUNT 6

AI in rechtshandhaving

Risicobeoordeling, bewijs en opsporing, zorgvuldig en uitlegbaar.

Risicobeoordeling | Bewijsbetrouwbaarheid | Menselijk toezicht | Grondrechten

Juridische peildatum: 2026-09-10 · Praktische gids, geen formeel juridisch advies.

VOORWOORD VAN DE EXPERT

AI in rechtshandhaving.

AI in rechtshandhaving raakt direct aan de fundamentele rechten van burgers: vrijheid, gelijke behandeling, het vermoeden van onschuld en bescherming van persoonsgegevens.

Zahed Ashkara begeleidt organisaties van AI Act-plicht naar review-klaar bewijs. Dit rapport bundelt die aanpak per domein, zodat uw inzet uitlegbaar en onderbouwd is richting toezichthouder en klant.

Wat dit rapport wel is

- Een praktische readiness-gids per domein of route
- Een uitleglaag bij de relevante AI Act-artikelen
- Een raamwerk om bewijs op te bouwen

Wat dit rapport niet is

- Formeel juridisch advies of conformiteitsbeoordeling
- Een vervanging van DPIA, FRIA of vendor due diligence
- Een garantie van compliance

INHOUDSOPGAVE

Wat u in dit rapport vindt.

01 Executive summary

02 De plaats van rechtshandhaving in de risicopiramide

03 Wat Annex III punt 6 precies aanwijst als hoog-risico

04 De verboden toepassingen: de harde ondergrens van Artikel 5

05 Kernverplichtingen voor hoog-risico opsporingssystemen

06 Menselijk toezicht, uitlegbaarheid en het vermoeden van onschuld

07 Governance, leverancier en handhaving

08 De verplichtingen op een rij

09 Evidence pack: de checklist

10 Stappenplan: 30, 60, 90 dagen

11 Veelgestelde vragen

12 Over de expert

KERNPUNTEN

AI in rechtshandhaving.

AI in rechtshandhaving raakt direct aan de fundamentele rechten van burgers: vrijheid, gelijke behandeling, het vermoeden van onschuld en bescherming van persoonsgegevens. Daarom plaatst de EU AI-verordening (Verordening (EU) 2024/1689) een aanzienlijk deel van de toepassingen die politie, openbaar ministerie en opsporingsdiensten gebruiken in Annex III punt 6: de categorie hoog-risico AI-systemen met de zwaarste verplichtingen. Het gaat onder meer om systemen die het risico inschatten dat iemand slachtoffer of dader wordt, om polygraaf-achtige tools, om het beoordelen van de betrouwbaarheid van bewijs en om profilering van personen tijdens opsporing en vervolging.

Peildatum 10 september 2026. Verordening (EU) 2026/1744 is in werking. De plichten uit Hoofdstuk III, secties 1 tot en met 3, voor hoog-risico AI onder Artikel 6(2) en Annex III gelden vanaf 2 december 2027, behoudens de uitzondering voor Artikel 6(5). Toets voor bestaande systemen afzonderlijk het overgangsrecht van Artikel 111. Artikel 4 en toepasselijke verboden gelden al; toepasselijke Artikel 50-plichten gelden sinds 2 augustus 2026. Voor lid 2 geldt alleen voor systemen die vóór 2 augustus 2026 op de markt waren een overgang tot 2 december 2026.

BEVINDING 01

De plaats van rechtshandhaving in de risicopiramide

De EU AI-verordening hanteert een risicogebaseerde opzet met vier niveaus: onaanvaardbaar risico (verboden), hoog risico, beperkt risico (transparantieplichten) en minimaal risico.

BEVINDING 02

Wat Annex III punt 6 precies aanwijst als hoog-risico

Annex III punt 6 somt vijf categorieen op, telkens voor zover de inzet onder toepasselijk recht is toegestaan.

BEVINDING 03

De verboden toepassingen: de harde ondergrens van Artikel 5

Artikel 5 lid 1 onder (d) verbiedt risicobeoordelingen die uitsluitend op basis van profilering of het beoordelen van persoonlijkheidskenmerken voorspellen dat iemand een strafbaar feit zal plegen.

BEVINDING 04

Kernverplichtingen voor hoog-risico opsporingssystemen

Een aanbieder van een hoog-risico systeem moet een risicomanagementsysteem inrichten dat de hele levenscyclus omspant (Artikel 9), met databeheer dat de kwaliteit en representativiteit van trainings-, validatie- en testdata borgt (Artikel 10).

IN CONTEXT

Uw route door de AI Act.

Annex III punt 6	2 dec 2027	6	30 / 60 / 90
ONDERWERP	ANNEX III: HFD. III, SECTIES 1-3	AANDACHTSPUNTEN	PLANRITME IN DAGEN

Dit betreft de plichten voor systemen onder artikel 6 lid 2 en Annex III, met uitzondering van artikel 6 lid 5. Onderzoek eerst classificatie en eventuele overgangsregels van artikel 111. Artikel 4, artikel 5 en artikel 50 kunnen al gelden.

DE RISICOPIRAMIDE VAN DE AI ACT

Schematische routes, geen afzonderlijke hokjes: artikel 50 kan ook gelden voor een hoog-risicosysteem. Hoofdstuk V bevat een aparte route voor GPAI-modelaanbieders. Begin steeds bij het werkelijke gebruik en uw rol.

DE TIJDLIJN VAN DE VERORDENING

2 feb 2025	Verboden praktijken en AI-geletterdheid
2 aug 2025	GPAI-modelplichten; bestaande modellen: zie overgang
27 jul 2026	Omnibus in werking; gewijzigde AI-geletterdheidsplicht
2 aug 2026	Artikel 50 geldt; GPAI-handhaving actief
2 dec 2026	Einde overgang art. 50(2), alleen systemen vóór 2 aug 2026
2 aug 2027	GPAI-modellen op de markt vóór 2 aug 2025
2 dec 2027	Hoofdstuk III, secties 1-3: art. 6(2) / Annex III
2 aug 2028	Hoofdstuk III, secties 1-3: art. 6(1) / Annex I

Hoofdstuk III: uitzondering voor artikel 6 lid 5. Controleer per systeem ook artikel 111. Dit overzicht is geen uniforme deadline voor alle AI.

VAN PLICHT NAAR BEWIJS

Classificatie › **Risicobeheer** › **Documentatie en logging** › **Menselijk toezicht** › **Evidence pack**

WIE DRAAGT WELKE PLICHT

Onderstaande verdeling betreft hoog-risicosystemen, voor zover de genoemde plicht geldt. Classificatie, rol en overgang bepalen de uitkomst.

Aanbieder (provider)

Ontwikkelt of laat ontwikkelen en brengt onder eigen naam op de markt of stelt in gebruik

- Hoofdstuk III: risicobeheer, data en documentatie (Art. 9 tot 15)
- Conformiteitsbeoordeling en CE-markering
- Registratie volgens Art. 49: EU of nationaal, waar van toepassing

Gebruiksverantwoordelijke (deployer)

Zet het systeem in onder eigen gezag

- Gebruik conform instructies en monitoring (Art. 26)
- Menselijk toezicht en logs bewaren
- Grondrechtenassessment waar vereist (Art. 27)

HOOFDSTUK 02

De plaats van rechtshandhaving in de risicopiramide

De EU AI-verordening hanteert een risicogebaseerde opzet met vier niveaus: onaanvaardbaar risico (verboden), hoog risico, beperkt risico (transparantieplichten) en minimaal risico. Rechtshandhaving valt grotendeels in de twee zwaarste niveaus. Annex III punt 6 wijst specifieke opsporings- en risicobeoordelingstoepassingen aan als hoog-risico, terwijl Artikel 5 een aantal politiële toepassingen volledig verbiedt.

Het onderscheid is principieel. Een hoog-risico systeem mag worden ingezet, maar alleen onder strikte waarborgen en met volledige documentatie. Een verboden toepassing mag in het geheel niet worden gebouwd, in de handel gebracht of gebruikt, ongeacht de waarborgen die de aanbieder eromheen zet. Voor een opsporingsdienst is dit eerste vraagstuk dus geen technische maar een juridische classificatievraag: zit deze use case boven of onder de verbodsgrens?

Belangrijk is dat de verordening de bestaande bevoegdheidskaders niet vervangt. Een AI-systeem mag alleen worden ingezet voor zover de onderliggende politiële of justitiële taak op grond van Unierecht of nationaal recht is toegestaan. De AI-verordening stapelt verplichtingen bovenop die grondslag, zij vervangt die niet.

VOORBEELD UIT DE PRAKTIJK

Een politiekorps wil een tool aanschaffen die per verdachte een recidiverisicoscore berekent ter ondersteuning van een beslissing over voorlopige hechtenis. Dit valt onder Annex III punt 6 (d): risicobeoordeling van her- of opnieuw plegen. Het systeem is toegestaan, maar uitsluitend als hoog-risico systeem met volledige documentatie, menselijk toezicht en een grondrechtenassessment. Zou dezelfde score puur op basis van profilering voorspellen of iemand uberhaupt een strafbaar feit gaat plegen, dan kantelt het naar het verbod van Artikel 5.

HOOFDSTUK 03

Wat Annex III punt 6 precies aanwijst als hoog-risico

Annex III punt 6 somt vijf categorieen op, telkens voor zover de inzet onder toepasselijk recht is toegestaan. Punt (a) betreft systemen die het risico inschatten dat een natuurlijke persoon slachtoffer wordt van strafbare feiten. Punt (b) betreft AI die functioneert als polygraaf of vergelijkbaar instrument. Deze categorieen raken direct aan betrouwbaarheid en aan de positie van kwetsbare personen.

Punt (c) ziet op het beoordelen van de betrouwbaarheid van bewijs in het kader van onderzoek of vervolging. Dit is gevoelig omdat de uitkomst rechtstreeks doorwerkt in de bewijswaardering en daarmee in het recht op een eerlijk proces. Punt (d) betreft het inschatten van het risico dat iemand een strafbaar feit pleegt of herhaalt, mede op basis van persoonlijkheidskenmerken of eerder strafrechtelijk gedrag, voor zover dit niet onder het verbod van Artikel 5 valt.

Punt 6(e) betreft profilering van natuurlijke personen tijdens opsporing, onderzoek of vervolging van strafbare feiten. Toets bij ieder subpunt eerst of het gebruik rechtmatig is en precies binnen de omschrijving valt. Alleen daarna volgt de eventuele uitzondering van Artikel 6(3); die is niet beschikbaar bij profilering. De plichten worden vervolgens aan de juiste actor en toepassingsdatum gekoppeld.

HOOFDSTUK 04

De verboden toepassingen: de harde ondergrens van Artikel 5

Artikel 5 lid 1 onder (d) verbiedt risicobeoordelingen die uitsluitend op basis van profilering of het beoordelen van persoonlijkheidskenmerken voorspellen dat iemand een strafbaar feit zal plegen. De grens ligt bij menselijke beoordeling die berust op objectieve en verifieerbare feiten die rechtstreeks met een strafbare activiteit verband houden: een systeem dat zo'n menselijke beoordeling ondersteunt valt buiten het verbod.

Artikel 5 lid 1 onder (e) verbiedt het ongericht verzamelen (scrapen) van gezichtsafbeeldingen van internet of CCTV om gezichtsherkenningsdatabases op te bouwen of uit te breiden. Onder (g) is biometrische categorisatie verboden die ras, politieke opvattingen, vakbondslidmaatschap, religieuze of levensbeschouwelijke overtuiging, seksleven of seksuele gerichtheid afleidt, met een beperkte uitzondering voor het labelen van rechtmatig verkregen biometrische datasets.

Artikel 5 lid 1 onder (h) verbiedt real-time biometrische identificatie op afstand in publiek toegankelijke ruimten voor rechtshandhaving, behoudens eng omschreven uitzonderingen: het zoeken naar slachtoffers van bepaalde misdrijven of vermiste personen, het voorkomen van een concrete dreiging voor het leven of een terroristische aanslag, en het lokaliseren van verdachten van ernstige strafbare feiten. De leden 2 en 3 eisen voor die uitzonderingen voorafgaande rechterlijke of bestuurlijke toestemming en een grondrechtenimpactassessment.

VOORBEELD UIT DE PRAKTIJK

Een gemeente overweegt camerasystemen met live gezichtsherkenning op een uitgaansplein om verdachten automatisch te identificeren. Dit is real-time biometrische identificatie op afstand in een publiek toegankelijke ruimte en valt onder het verbod van Artikel 5 lid 1 onder (h). Inzet kan alleen binnen de eng omschreven uitzonderingen, met voorafgaande rechterlijke of bestuurlijke toestemming per inzet en een grondrechtenassessment. Permanente, generieke surveillance van het plein is niet toegestaan.

HOOFDSTUK 05

Kernverplichtingen voor hoog-risico opsporingssystemen

Een aanbieder van een hoog-risico systeem moet een risicomanagementsysteem inrichten dat de hele levenscyclus omspant (Artikel 9), met databeheer dat de kwaliteit en representativiteit van trainings-, validatie- en testdata borgt (Artikel 10). Juist in rechtshandhaving is dit cruciaal: vertekening in historische opsporingsdata kan groepen stelselmatig benadelen en discriminatie reproduceren.

Daarnaast gelden verplichtingen rond technische documentatie (Artikel 11), automatische logging van gebeurtenissen (Artikel 12), transparantie richting de gebruiksverantwoordelijke (Artikel 13), effectief menselijk toezicht (Artikel 14) en een passend niveau van nauwkeurigheid, robuustheid en cybersecurity (Artikel 15). Het systeem moet voor inzet zijn voorzien van een conformiteitsbeoordeling en CE-markering, en worden geregistreerd in de EU-databank.

De gebruiksverantwoordelijke (deployer), doorgaans de opsporingsdienst zelf, draagt eigen verplichtingen (Artikel 26): gebruik conform de instructies, monitoring, bewaren van logs en het inschakelen van menselijk toezicht. Voor veel publieke deployers geldt bovendien de plicht tot een grondrechtenimpactassessment voordat het systeem in gebruik wordt genomen (Artikel 27).

HOOFDSTUK 06

Menselijk toezicht, uitlegbaarheid en het vermoeden van onschuld

Menselijk toezicht is in de opsporingscontext niet alleen een nalevingsvereiste maar een rechtsstatelijke noodzaak. Artikel 14 eist dat een mens de output kan begrijpen, kan negeren of terugdraaien en automation bias kan herkennen. Een risicoscore of profileringsuitkomst mag nooit de feitelijke beslissing nemen; zij ondersteunt een beslissing die door een bevoegde functionaris wordt genomen en gemotiveerd.

Dit hangt samen met het vermoeden van onschuld en het recht op een eerlijk proces. Een betrouwbaarheidsbeoordeling van bewijs of een recidivescore die ondoorzichtig tot stand komt, ondermijnt de mogelijkheid van de verdediging om de uitkomst te toetsen. Uitlegbaarheid en reproduceerbaarheid van de output zijn daarom geen luxe, maar voorwaarde voor toelaatbaarheid in de procedure.

Praktisch betekent dit dat elke ingrijpende uitkomst herleidbaar moet zijn tot de gebruikte input, het model en de menselijke afweging. Logging (Artikel 12) levert het bewijs dat het toezicht ook daadwerkelijk is uitgeoefend, en is daarmee de ruggengraat van verantwoording achteraf.

HOOFDSTUK 07

Governance, leverancier en handhaving

De verantwoordelijkheid is verdeeld over de keten. De aanbieder bouwt het systeem conform Hoofdstuk III; de deployer zet het rechtmatig in. Bij inkoop van een systeem van derden moet de opsporingsdienst contractueel borgen dat de leverancier de conformiteitsdocumentatie, logging-mogelijkheden en instructies levert die de deployer nodig heeft om aan zijn eigen verplichtingen te voldoen.

Niet-naleving kent stevige gevolgen. Het inzetten van een verboden toepassing kan via de toezichthouder leiden tot boetes tot 35 miljoen euro of 7 procent van de wereldwijde jaaromzet (Artikel 99). Voor schendingen van de hoog-risico verplichtingen liggen de maxima lager, maar nog steeds substantieel. Naast de boete via de toezichthouder staan bestuursrechtelijke gevolgen en reputatieschade. Voor kmo’s en start-ups geldt bij Artikel 99 het laagste maximum van bedrag en omzetpercentage, voor andere ondernemingen het hoogste; voor publieke instanties bepalen lidstaten of en in hoeverre boetes gelden.

Tijdlijn: het verbod uit Artikel 5 geldt sinds 2 februari 2025. Verordening (EU) 2026/1744 verplaatst de meeste zelfstandige hoog-risicoplichten uit Bijlage III naar 2 december 2027. Organisaties die opsporings-AI gebruiken of aanschaffen, doen er goed aan hun portfolio nu al tegen de toepasselijke kaders te toetsen.

De verplichtingen op een rij

1

Artikel 5 lid 1 onder (d) / (e) / (g) / (h)

Verboden toepassingen: predictive policing puur op profilering, ongericht scrapen van gezichtsafbeeldingen, biometrische categorisatie naar gevoelige kenmerken en real-time biometrische identificatie op afstand in de publieke ruimte (met eng omschreven uitzonderingen). Eerst toetsen of de use case boven of onder deze verbodsgrens zit.

2

Annex III punt 6 (a) tot (e)

Annex III punt 6 noemt specifieke opsporingstoepassingen. Toets de wettelijke omschrijving, toegelaten gebruik en Artikel 6(3); profilering sluit die uitzondering uit. Verdeel de toepasselijke Chapter III-plichten over aanbieder en deployer en koppel ze aan de juiste datum.

3

Artikel 9 / Artikel 10

De aanbieder richt risicomanagement en datagovernance in volgens Artikelen 9 en 10, met aandacht voor kwaliteit, representativiteit en bias. De deployer heeft eigen plichten rond gebruik, inputdata onder zijn controle en monitoring onder Artikel 26.

4

Artikel 11 / 12 / 13 / 14 / 15

De aanbieder borgt technische documentatie, logging, instructies, toezichtontwerp, nauwkeurigheid, robuustheid en cybersecurity. De deployer organiseert bevoegd menselijk toezicht. Bij rechtshandhaving kunnen aanvullende specifieke beperkingen op uitsluitend geautomatiseerde besluiten gelden; toets de concrete toepassing en het toepasselijke gegevensbeschermingsrecht.

5

Artikel 26 / Artikel 27

Plichten van de gebruiksverantwoordelijke: gebruik conform instructies, monitoring, bewaren van logs en menselijk toezicht. Publieke deployers verrichten daarnaast een grondrechtenimpactassessment (FRIA) voordat het systeem in gebruik wordt genomen.

6

Artikel 49 / Artikel 99

Registratie van het hoog-risico systeem in de EU-databank en handhaving via de toezichthouder, met boetes tot 35 miljoen euro of 7 procent van de wereldwijde jaaromzet voor verboden toepassingen. Voor kmo’s en start-ups geldt bij Artikel 99 het laagste maximum van bedrag en omzetpercentage, voor andere ondernemingen het hoogste; voor publieke instanties bepalen lidstaten of en in hoeverre boetes gelden.

Evidence pack: de checklist

- Classificatiebeslissing per use case vastgelegd: verboden (Artikel 5), hoog-risico (Annex III punt 6) of lager, met juridische onderbouwing
- Rechtsgrondslag voor de onderliggende opsporings- of risicobeoordelingstaak in Unierecht of nationaal recht aangetoond
- Grondrechtenimpactassessment (FRIA) uitgevoerd en gedateerd voor ingebruikname (Artikel 27)
- Databeheerdossier met herkomst, kwaliteit, representativiteit en bias-analyse van trainings-, validatie- en testdata (Artikel 10)
- Technische documentatie en conformiteitsbeoordeling met CE-markering, plus registratie in de EU-databank (Artikel 11, 43, 49)
- Logbestanden die aantonen dat menselijk toezicht is uitgeoefend en dat output herleidbaar en uitlegbaar is (Artikel 12, 14)
- Inkoop- en verwerkersafspraken met de leverancier over documentatie, logging-toegang en gebruiksinstructies
- Procedure voor uitlegbaarheid richting verdediging en rechter, met reproduceerbaarheid van individuele uitkomsten

Stappenplan: 30, 60, 90 dagen

Indicatief planritme. De haalbaarheid hangt af van scope, bestaande maatregelen en beschikbaar bewijs.

0 tot 30 dagen

- Inventariseer alle AI-systemen in opsporing, risicobeoordeling en bewijsketen en breng leveranciers in kaart
- Voer per systeem een eerste classificatie uit: verboden, hoog-risico of lager
- Markeer direct alle toepassingen die mogelijk onder het verbod van Artikel 5 vallen en bevries inzet zolang de toets loopt

30 tot 60 dagen

- Voer per hoog-risico systeem een gap-analyse uit tegen de verplichtingen van Hoofdstuk III (Artikel 9 tot 15)
- Start de grondrechtenimpactassessments (FRIA) voor systemen die in gebruik zijn of binnenkort worden aangeschaft
- Beoordeel data-kwaliteit en bias en leg het databeheerdossier aan; controleer of leveranciers de benodigde documentatie kunnen leveren

60 tot 90 dagen

- Richt menselijk toezicht, logging en uitlegbaarheidsprocedures operationeel in en test ze
- Verwerk de vereisten in inkoop- en verwerkerscontracten en in de conformiteits- en registratiedossiers
- Stel een doorlopend governance- en monitoringritme vast met duidelijk eigenaarschap, gericht op de toepasselijke Annex III-datum van 2 december 2027

Veelgestelde vragen

Mag predictive policing nog onder de verordening?

Niet als de voorspelling uitsluitend berust op profilering of het beoordelen van persoonlijkheidskenmerken: dat is verboden onder Artikel 5 lid 1 onder (d). Een systeem dat een menselijke beoordeling ondersteunt die berust op objectieve, verifieerbare feiten die rechtstreeks met een strafbare activiteit verband houden, valt buiten het verbod en wordt dan als hoog-risico behandeld.

Is live gezichtsherkenning op straat door de politie toegestaan?

Artikel 5(1)(h) betreft real-time biometrische identificatie op afstand in publiek toegankelijke ruimten voor rechtshandhaving. Alleen de nauw omschreven wettelijke doelen en waarborgen kunnen een uitzondering dragen, waaronder een FRIA en in beginsel voorafgaande toestemming van een rechterlijke of bindend beslissende onafhankelijke administratieve autoriteit. Bij naar behoren gemotiveerde spoed kan een verzoek binnen 24 uur volgen; bij afwijzing moet het gebruik stoppen en moeten de relevante gegevens worden verwijderd.

Valt een systeem dat de betrouwbaarheid van bewijs beoordeelt onder de zwaarste categorie?

Annex III punt 6(c) noemt AI voor de beoordeling van de betrouwbaarheid van bewijs bij onderzoek of vervolging van strafbare feiten. Toets de exacte functie en Artikel 6(3), naast de rechtmatigheid van het gebruik. Bij hoog-risicokwalificatie gelden de aan de betreffende actor gekoppelde plichten vanaf de toepasselijke datum.

Wie is verantwoordelijk, de leverancier of de opsporingsdienst?

Beide. De aanbieder bouwt het systeem conform Hoofdstuk III (conformiteit, documentatie, logging-mogelijkheden). De opsporingsdienst is gebruiksverantwoordelijke (Artikel 26) en moet het rechtmatig inzetten, monitoren, logs bewaren en menselijk toezicht borgen, en in de regel een grondrechtenassessment uitvoeren (Artikel 27).

Vanaf wanneer gelden deze regels?

Het verbod uit Artikel 5 geldt sinds 2 februari 2025. Verordening (EU) 2026/1744 verplaatst de meeste zelfstandige hoog-risicoplichten uit Bijlage III naar 2 december 2027. Toets het portfolio ruim voor die datum en breng de governance op orde.

OVER DE EXPERT

Zahed Ashkara

AI Act consultant · AI governance specialist · jurist en spreker

Zahed Ashkara adviseert organisaties over de EU AI Act, de AVG en verantwoorde AI-adoptie, en overbrugt Legal, IT en Business. Als spreker en consultant vertaalt hij complexe wetgeving naar concrete, aantoonbare stappen: van classificatie tot een review-klaar evidence pack. Hij is oprichter van Embed AI en Praxikon.

> **Compliance onder de AI Act is geen technologievraag, maar een classificatie- en bewijsvraag. Begin bij de juiste classificatie, niet bij het model.**

Over Embed AI

Embed AI maakt AI in organisaties verantwoord en klantklaar onder de EU AI Act en de AVG. Van onafhankelijke risk check en classificatie tot een review-klaar evidence pack, juridisch en technisch, met implementatie. Voor organisaties met AI in hun processen en vendors die AI verkopen.

Bronnen en vervolgstap

Versie 2026.09 · Peildatum 2026-09-10

Dit rapport verwijst naar de officiele tekst van Verordening (EU) 2024/1689 en de richtsnoeren van de Europese Commissie. Lees de officiële bronnen samen met de wijzigingen. Praxikon biedt aanvullende uitleg per domein.

EU AI Act: Verordening (EU) 2024/1689

Digital Omnibus on AI: Regulation (EU) 2026/1744, Article 1(39)-(40)

European Commission: implementation timeline

Wijziging AI Act: Verordening (EU) 2026/1744

Commission draft guidelines: high-risk classification (19 May 2026)

Praxikon · Actuele rapporten

Neem uw toepassing en de open vraag over verbodsgrenzen, rol of bewijs mee naar de AI Act gap-intake. Embed AI helpt het open punt afbakenen en een passende vervolgstap bepalen.

Bespreek uw open punt