THE AI CONTENT ENGINEER

EU AI Act
Volledige Wetgeving

Verordening (EU) 2024/1689 — Kunstmatige Intelligentie

JURIDISCHE REFERENTIE & COMPLIANCE GIDS

Samengesteld door
The AI Content Engineer

Publicatie 2024 | Versie 1.0

Inhoudsopgave

Samenvatting

Verordening (EU) 2024/1689 — de **Artificial Intelligence Act (AI Act)** — is op **13 juni 2024** vastgesteld door het Europees Parlement en de Raad en op **12 juli 2024** gepubliceerd in het Publicatieblad van de Europese Unie. Het is het eerste horizontale, sectoroverschrijdende rechtskader ter wereld voor kunstmatige intelligentie en steunt op een **risicogebaseerde benadering**: hoe hoger het risico dat een AI-systeem voor gezondheid, veiligheid of grondrechten oplevert, hoe strenger de verplichtingen. De verordening verbiedt een aantal onaanvaardbare AI-praktijken, stelt zware eisen aan hoog-risico AI-systemen, legt transparantieverplichtingen op aan bepaalde systemen (waaronder generatieve AI), en introduceert een apart regime voor AI-modellen voor algemene doeleinden (GPAI) en modellen met systeemrisico.

De verordening is in werking getreden op **1 augustus 2024**, met een **gefaseerde toepassing** waarvan het merendeel van de kernverplichtingen geldt vanaf **2 augustus 2026** en het volledige kader vanaf **2 augustus 2027**.

Voor organisaties die bij AI Act-compliance worden ondersteund, zijn drie zaken bepalend. Ten eerste is de reikwijdte **extraterritoriaal**: de regels gelden ook voor aanbieders en gebruikers buiten de Unie zodra de output van hun AI-systeem in de Unie wordt gebruikt. Ten tweede concentreert de nalevingslast zich op **hoog-risico AI-systemen**, waarvoor de artikelen 9 t/m 15 een cumulatief pakket aan verplichtingen opleggen — risicomanagement, datagovernance, technische documentatie, logging, transparantie, menselijk toezicht en accuraatheid/robuustheid/cyberbeveiliging. Ten derde is het handhavingskader met **administratieve boetes** onder artikel 99 ontworpen om "doeltreffend, evenredig en afschrikkend" te zijn.

Dit document dient als interne naslagreferentie op basis van de officiële EUR-Lex/Publicatieblad-tekst van Verordening (EU) 2024/1689. Het reproduceert de wettelijke structuur per thema — doel en toepassingsgebied, definities, verboden praktijken, risicoclassificatie, verplichtingen voor de gehele waardeketen, GPAI-regime, conformiteitsbeoordeling, governance, meldplicht en sancties, tijdlijn en bijlagen — en behoudt waar mogelijk de juridische formulering.

> **Kernboodschap voor besluitvormers:** De AI Act is een bindend, direct werkend Unierecht met een gefaseerde tijdlijn die nu al loopt. Organisaties moeten hun AI-systemen classificeren (verboden / hoog-risico / transparantie / minimaal), de zwaartepunten leggen bij hoog-risico-verplichtingen (art. 9-15) en GPAI-verplichtingen, en een compliance-programma opzetten dat de mijlpalen van augustus 2025, 2026 en 2027 haalt.

Belangrijkste Bevindingen

1. **De AI Act is definitief vastgesteld, gepubliceerd en van kracht.** De verordening is aangenomen op 13 juni 2024, gepubliceerd op 12 juli 2024 en in werking getreden op 1 augustus 2024. *So what:* Compliance is geen toekomstscenario maar een lopende juridische verplichting; organisaties die wachten op "definitieve duidelijkheid" lopen achter op een tijdlijn die al is begonnen.

2. **De verordening hanteert vier risicoklassen.** AI-systemen worden ingedeeld in onaanvaardbaar risico (verboden), hoog risico, transparantierisico en minimaal/geen risico. *So what:* De eerste, goedkoopste compliance-stap is een correcte classificatie — die bepaalt of een systeem verboden is, zwaar gereguleerd, licht gereguleerd of vrij van verplichtingen.

3. **De reikwijdte is extraterritoriaal.** De regels gelden voor aanbieders binnen én buiten de Unie en voor gebruikers in de Unie, en zelfs voor derde-landaanbieders wanneer de output in de Unie wordt gebruikt. *So what:* Niet-EU-technologieleveranciers en hun EU-klanten moeten beide beoordelen of zij onder de verordening vallen; contractuele ketenafspraken worden cruciaal.

4. **Hoog-risico-verplichtingen zijn cumulatief en zwaar.** De artikelen 9-15 vereisen een risicomanagementsysteem, datagovernance, technische documentatie, automatische logging, transparantie richting gebruikers, menselijk toezicht en passende accuraatheid, robuustheid en cyberbeveiliging. *So what:* Voor een hoog-risico-systeem is niet één, maar het volledige pakket van verplichtingen tegelijk vereist — compliance vergt een integraal kwaliteits- en documentatiesysteem, geen losse maatregelen.

5. **Bepaalde AI-praktijken zijn volledig verboden.** Manipulatie, uitbuiting van kwetsbaarheden, social scoring, ongerichte scraping van gezichtsbeelden, emotieherkenning op werk/onderwijs en (met uitzonderingen) real-time biometrische identificatie in openbare ruimten voor rechtshandhaving. *So what:* Deze praktijken kunnen niet met documentatie of toezicht "compliant" worden gemaakt; ze moeten uit de productportefeuille worden verwijderd.

6. **GPAI-modellen kennen een apart, tweeledig regime.** Alle aanbieders van AI-modellen voor algemene doeleinden hebben transparantie- en documentatieverplichtingen; modellen met **systeemrisico** hebben aanvullende verplichtingen. Een drempel gebaseerd op cumulatieve rekenkracht (floating point operations) leidt tot een vermoeden van systeemrisico. *So what:* Ontwikkelaars van grote modellen en downstream-integrators moeten in kaart brengen of zij als GPAI-aanbieder kwalificeren en of de systeemrisico-drempel wordt gehaald.

7. **De governance is centraal én nationaal georganiseerd.** Het **AI Office** binnen de Commissie en de **European Artificial Intelligence Board** coördineren de uitvoering, ondersteund door een wetenschappelijk panel van maximaal 60 onafhankelijke experts. *So what:* Handhaving en interpretatie zullen zich concentreren rond het AI Office (vooral voor GPAI) en nationale autoriteiten; organisaties moeten weten wie hun bevoegde toezichthouder is.

8. **Meldplicht bij ernstige incidenten en zware boetes onder artikel 99.** Aanbieders (en gebruikers) moeten ernstige incidenten melden aan markttoezichtautoriteiten; boetes moeten doeltreffend, evenredig en afschrikkend zijn. *So what:* Een incident-response- en meldproces moet vóór ingebruikname operationeel zijn, niet erna.

9. **De tijdlijn is gefaseerd over meerdere jaren.** Verboden en definities golden vanaf 2 februari 2025, governance en GPAI vanaf 2 augustus 2025, de meeste hoog-risico-eisen vanaf 2 augustus 2026, en het volledige kader vanaf 2 augustus 2027. *So what:* Roadmaps moeten aan deze kalender worden verankerd; verschillende verplichtingen worden op verschillende data afdwingbaar.

10. **Er lopen voorstellen tot vereenvoudiging ("Digital Omnibus on AI").** In november 2025 stelde de Commissie COM/2025/836 voor om implementatie te vereenvoudigen, onder meer door hoog-risico-tijdlijnen te koppelen aan de beschikbaarheid van standaarden en simplificaties uit te breiden naar kleine mid-caps. *So what:* De regels zijn nog in beweging; compliance-programma's moeten flexibel genoeg zijn om aanpassingen op te vangen, maar de kernverplichtingen blijven overeind.

> **Bottom line:** De AI Act is een breed, gelaagd en handhaafbaar kader. De grootste compliance-investering ligt bij correcte classificatie, het volledige hoog-risico-pakket (art. 9-15), het GPAI-regime en een meld- en governance-infrastructuur die op de gefaseerde tijdlijn is afgestemd.

Gedetailleerde Analyse

De volgende vijftien thema's behandelen de EU AI Act systematisch, van juridische grondslag tot praktische toepassing. Per thema wordt de kern van de wettelijke vereisten uiteengezet, gevolgd door een strategische conclusie voor compliance-besluitvormers.

1. Doel, aard en juridische grondslag

Het doel van de verordening is het verbeteren van de werking van de interne markt door een uniform rechtskader vast te leggen voor de ontwikkeling, het in de handel brengen, de ingebruikneming en het gebruik van AI-systemen in de Unie, in overeenstemming met de waarden van de Unie. Het kader beoogt de opname van **mensgerichte en betrouwbare AI** te bevorderen en tegelijk een hoog niveau van bescherming te waarborgen van gezondheid, veiligheid en grondrechten zoals verankerd in het Handvest van de grondrechten van de Europese Unie — inclusief democratie, de rechtsstaat en milieubescherming. De verordening waarborgt het vrije, grensoverschrijdende verkeer van AI-gebaseerde goederen en diensten en verhindert dat lidstaten beperkingen opleggen aan de ontwikkeling, marketing en het gebruik van AI-systemen, tenzij uitdrukkelijk toegestaan door de verordening.

De verordening moet worden toegepast in overeenstemming met de waarden van de Unie zoals verankerd in het Handvest, ter bescherming van natuurlijke personen, ondernemingen, democratie, de rechtsstaat en het milieu, terwijl innovatie en werkgelegenheid worden gestimuleerd. Als voorwaarde geldt dat AI een **mensgerichte technologie** moet zijn: een instrument ten dienste van mensen, met als uiteindelijk doel het verhogen van het menselijk welzijn.

De verordening is primair gebaseerd op **artikel 114 VWEU** (interne markt). Voor zover zij specifieke regels bevat over de verwerking van persoonsgegevens — beperkingen op het gebruik van AI-systemen voor biometrische identificatie op afstand voor rechtshandhaving, voor risicobeoordelingen van natuurlijke personen voor rechtshandhaving en voor biometrische categorisering voor rechtshandhaving — is zij ook gebaseerd op **artikel 16 VWEU**.

De AI Act is **complementair** aan bestaand Unierecht. Zij laat onverlet: gegevensbescherming (waaronder de AVG, Verordening (EU) 2016/679, en Verordening (EU) 2018/1725, en Richtlijn (EU) 2016/680), consumentenbescherming, grondrechten, werkgelegenheid en de bescherming van werknemers, en productveiligheid. Alle rechten en rechtsmiddelen die dergelijk Unierecht biedt aan consumenten en andere personen op wie AI-systemen een negatief effect kunnen hebben — inclusief schadevergoeding — blijven onverkort van toepassing.

> **Bottom line:** De AI Act is interne-marktwetgeving met een grondrechten- en veiligheidskern. Zij vervangt bestaand recht niet maar stapelt er bovenop; compliance-analyses moeten de AI Act altijd naast AVG, productveiligheid en sectorregels lezen.

2. Toepassingsgebied en uitzonderingen

De verordening is van toepassing op **aanbieders** van AI-systemen op niet-discriminatoire wijze, ongeacht of zij binnen de Unie of in een derde land zijn gevestigd, en op **gebruikers (deployers)** van AI-systemen die in de Unie zijn gevestigd. Cruciaal voor de reikwijdte is dat de verordening ook van toepassing is op aanbieders en gebruikers die in een derde land zijn gevestigd, **voor zover de output** van hun systemen bestemd is om in de Unie te worden gebruikt. Dit voorkomt omzeiling: een in de Unie gevestigde operator kan bijvoorbeeld diensten uitbesteden aan een operator in een derde land die een hoog-risicoactiviteit uitvoert met in de Unie verzamelde data en de output aan de contracterende operator in de Unie levert. De verordening is eveneens van toepassing op instellingen, organen en instanties van de Unie wanneer zij optreden als aanbieder of gebruiker.

De belangrijkste **uitzonderingen** op de reikwijdte zijn:

- **Militaire, defensie- en nationale-veiligheidsdoeleinden.** AI-systemen die uitsluitend voor deze doeleinden in de handel worden gebracht, in gebruik worden genomen of worden gebruikt, vallen buiten de verordening, ongeacht het type entiteit. Als een dergelijk systeem echter (tijdelijk of permanent) voor andere doeleinden wordt gebruikt — bijvoorbeeld civiele, humanitaire of rechtshandhavingsdoeleinden — valt het wél binnen de reikwijdte.
- **Wetenschappelijk onderzoek en ontwikkeling.** AI-systemen en -modellen die specifiek en uitsluitend voor wetenschappelijk onderzoek en ontwikkeling worden ontwikkeld en in gebruik genomen, vallen buiten de verordening. Dit laat de verplichting onverlet om de verordening na te leven zodra een systeem daadwerkelijk in de handel wordt gebracht of in gebruik wordt genomen.
- **Publieke autoriteiten van derde landen en internationale organisaties** die optreden in het kader van samenwerking of internationale overeenkomsten voor rechtshandhaving en justitiële samenwerking, mits passende waarborgen voor grondrechten bestaan.
- **Vrije en openbroncomponenten.** Derden die tools, diensten, processen of AI-componenten (anders dan GPAI-modellen) onder een vrije en openbronlicentie toegankelijk maken, zijn niet verplicht te voldoen aan de waardeketen-verplichtingen. Deze uitzondering geldt echter niet wanneer componenten gemonetariseerd worden aangeboden.

> **Bottom line:** De reikwijdte is breed en extraterritoriaal. Organisaties buiten de EU met EU-output vallen eronder; de uitzonderingen (defensie, zuiver onderzoek, open source) zijn nauw omschreven en moeten per geval worden getoetst.

3. Definities en kernbegrippen

De verordening definieert het begrip **"AI-systeem"** zo dat het nauw aansluit bij het werk van internationale organisaties, voor rechtszekerheid en internationale convergentie, met flexibiliteit voor snelle technologische ontwikkelingen. Een sleutelkenmerk is het **vermogen om te concluderen (infer)**: het proces van het verkrijgen van outputs zoals voorspellingen, content, aanbevelingen of beslissingen die fysieke en virtuele omgevingen kunnen beïnvloeden, en het vermogen om modellen of algoritmen af te leiden uit inputs of data. Technieken die

conclusie mogelijk maken omvatten machine-learningbenaderingen en logica- en kennisgebaseerde benaderingen. AI-systemen zijn ontworpen om te functioneren met **variërende niveaus van autonomie** en kunnen **aanpassingsvermogen (adaptiveness)** vertonen na deployment.

Begrip	Kern van de definitie
Deployer (gebruiker)	Elke natuurlijke of rechtspersoon, inclusief overheidsinstantie, die een AI-systeem onder zijn gezag gebruikt, behalve bij persoonlijk niet-professioneel gebruik
Biometrische gegevens	Maken authenticatie, identificatie of categorisering en emotieherkenning mogelijk; uit te leggen in het licht van de AVG en Richtlijn (EU) 2016/680
Biometrische identificatie	Geautomatiseerde herkenning van fysieke, fysiologische en gedragskenmerken om identiteit vast te stellen door vergelijking met een referentiedatabase
Biometrische categorisering	Indeling van natuurlijke personen in categorieën op basis van biometrische gegevens (bijv. geslacht, leeftijd, haarkleur, gedrag)
Emotieherkenningssysteem	AI-systeem om emoties of intenties van natuurlijke personen te identificeren op basis van biometrische gegevens
Openbaar toegankelijke ruimte	Elke fysieke ruimte toegankelijk voor een onbepaald aantal personen; online ruimten vallen er niet onder

De verordening onderscheidt uitdrukkelijk **biometrische verificatie/authenticatie** (bevestigen dat iemand is wie hij beweert te zijn) van biometrische identificatie op afstand; verificatie valt buiten de zwaarste categorieën omdat die een geringer effect op grondrechten heeft. Het emotieherkenningsbegrip omvat emoties als geluk, verdriet, woede, verrassing en walging, maar **niet** fysieke toestanden zoals pijn of vermoeidheid (bijv. vermoeidheidsdetectie bij piloten of bestuurders ter voorkoming van ongevallen).

AI-geletterdheid (AI literacy) is een terugkerend concept: aanbieders, gebruikers en getroffen personen moeten voldoende begrip hebben om geïnformeerde beslissingen te nemen over AI-systemen. De zeven **ethische beginselen** van de High-Level Expert Group (AI HLEG) vormen een niet-bindende basis voor gedragscodes onder de verordening: menselijke controle en toezicht; technische robuustheid en veiligheid; privacy en datagovernance; transparantie; diversiteit, non-discriminatie en eerlijkheid; maatschappelijk en ecologisch welzijn; en verantwoordingsplicht.

> **Bottom line:** De brede, techniek-neutrale definitie van "AI-systeem" bepaalt de poort tot de hele verordening. De scheidslijnen — infer versus regelgebaseerde software, identificatie versus verificatie, emoties versus fysieke toestanden — zijn juridisch beslissend en moeten zorgvuldig worden gedocumenteerd.

4. Verboden AI-praktijken (onaanvaardbaar risico)

De verordening verbiedt bepaalde AI-praktijken omdat zij in strijd zijn met de waarden van de Unie inzake menselijke waardigheid, vrijheid, gelijkheid, democratie en de rechtsstaat en de grondrechten van het Handvest. De verboden praktijken krachtens artikel 5:

- **Manipulatieve of misleidende technieken.** AI-systemen die subliminale componenten (audio, beeld, video die personen niet kunnen waarnemen) of andere manipulatieve of misleidende technieken inzetten die de autonomie, besluitvorming of vrije keuze van personen ondermijnen, met als doel of gevolg het materieel verstoren van menselijk gedrag waardoor significante schade waarschijnlijk is. Het is niet vereist dat de aanbieder of gebruiker de intentie heeft om significante schade te veroorzaken, mits die schade voortvloeit uit de manipulatieve of uitbuitende praktijk.

- **Uitbuiting van kwetsbaarheden.** Het uitbuiten van kwetsbaarheden vanwege leeftijd, handicap of een specifieke sociale of economische situatie om gedrag materieel te verstoren op een wijze die significante schade veroorzaakt.

- **Social scoring.** Het evalueren of classificeren van natuurlijke personen of groepen op basis van sociaal gedrag of persoonlijke/persoonlijkheidskenmerken over bepaalde perioden, wat leidt tot nadelige of ongunstige behandeling in contexten die losstaan van de oorspronkelijke context of die disproportioneel of ongerechtvaardigd is.

- **Ongerichte scraping van gezichtsbeelden.** AI-systemen die gezichtsbeelddatabases aanmaken of uitbreiden door ongerichte scraping van gezichtsbeelden van internet of CCTV-beelden. "Ongericht" is hier het onderscheidende element: gericht verzamelen voor specifiek rechtmatig doel kan anders worden beoordeeld.

- **Emotieherkenning op werk en onderwijs.** AI-systemen die emoties van personen afleiden op de werkplek of in onderwijsinstellingen, behalve om medische of veiligheidsredenen. Dit verbod is absoluut voor de genoemde omgevingen; de uitzondering is nauw.

- **Biometrische categorisering op gevoelige kenmerken.** AI-systemen die individuen categoriseren op basis van biometrische gegevens in categorieën op basis van ras, politieke opvattingen, vakbondslidmaatschap, religieuze of filosofische overtuigingen, seksueel gedrag of seksuele geaardheid.

- **Real-time biometrische identificatie op afstand (RTBI) in openbare ruimten voor rechtshandhaving.** Gebruik van RTBI-systemen voor rechtshandhaving in openbaar toegankelijke ruimten is in beginsel verboden. De verordening voorziet in drie smalle uitzonderingen: (1) gericht zoeken naar bepaalde slachtoffers of vermiste personen; (2) voorkomen van een specifieke, substantiële en onmiddellijke dreiging voor leven of een terroristische aanslag; (3) opsporing, lokalisering, identificatie of strafrechtelijke vervolging van verdachten van specifieke strafbare feiten. Alle uitzonderingen vereisen voorafgaande rechterlijke of vergelijkbare toestemming (behoudens acute nood), zijn tijdelijk, geografisch beperkt en onderhevig aan democratisch toezicht.

> **Bottom line:** Verboden praktijken zijn compliant-proof: geen hoeveelheid documentatie, toezicht of waarborgen maakt ze acceptabel. De eerste prioriteit van elke compliance-scan is het uitsluiten van verboden toepassingen uit de portefeuille. Bijzondere aandacht is vereist voor RTBI, emotieherkenning en social-scoringsystemen die al in gebruik zijn.

5. Risicoclassificatie en hoog-risico AI-systemen

De verordening volgt een risicogebaseerde benadering met vier niveaus: **onaanvaardbaar risico** (verboden), **hoog risico**, **transparantierisico** en **minimaal of geen risico**. De zwaarste materiële eisen gelden voor hoog-risico AI-systemen. De classificatie als hoog risico verloopt via twee routes:

- **Annex I-route (artikel 6).** AI-systemen die veiligheidscomponenten zijn van producten, of zelf producten zijn, die vallen onder de in Annex I genoemde Unieharmonisatiewetgeving, en die onderworpen zijn aan een conformiteitsbeoordeling door een derde partij. Voorbeelden: machines, speelgoed, liften, radioapparatuur, medische hulpmiddelen, in-vitrodiagnostische medische hulpmiddelen, automotive en luchtvaart.
- **Annex III-route (stand-alone systemen).** Zelfstandige AI-systemen die, gezien hun beoogde doel, een hoog risico op schade voor gezondheid, veiligheid of grondrechten opleveren, gebruikt in specifiek vooraf gedefinieerde gebieden.

Annex III-gebied	Voorbeelden van hoog-risico use-cases
Biometrie	Biometrische identificatie op afstand; biometrische categorisering op gevoelige kenmerken; emotieherkenning (voor zover niet verboden)
Kritieke infrastructuur	Veiligheidscomponenten in beheer/exploitatie van kritieke digitale infrastructuur, wegverkeer en levering van water, gas, verwarming en elektriciteit
Onderwijs en beroepsopleiding	Toegang/toelating, toewijzing aan instellingen, evaluatie van leerresultaten, monitoring van verboden gedrag tijdens toetsen
Werkgelegenheid en arbeidsbeheer	Werving en selectie, beslissingen over arbeidsvoorwaarden, promotie/beëindiging, taaktoewijzing, monitoring en evaluatie

Essentiële particuliere en publieke diensten	Toegang tot overheidsvoorzieningen, kredietscoring, risicobeoordeling bij levens- en zorgverzekeringen, evaluatie van noodoproepen
Rechtshandhaving	Risicobeoordeling van slachtofferschap, polygrafen, beoordeling van bewijsbetrouwbaarheid, profilering bij opsporing
Migratie, asiel en grenscontrole	Risicobeoordeling van personen die binnenkomen, onderzoek van aanvragen, detectie/herkenning/identificatie
Rechtsbedeling en democratische processen	Systemen ter ondersteuning van rechterlijke autoriteiten; systemen om verkiezings- of referendumuitkomsten te beïnvloeden

De verordening voorziet in een belangrijke **uitzondering binnen Annex III**: een systeem in een van deze gebieden hoeft niet als hoog-risico te worden aangemerkt als het geen significant risico op schade oplevert omdat het de besluitvorming niet materieel beïnvloedt. Dit is het geval als aan een van de volgende voorwaarden is voldaan: (1) het systeem voert een enge procedurele taak uit; (2) het verbetert het resultaat van een eerder voltooide menselijke activiteit; (3) het detecteert besluitvormingspatronen of afwijkingen zonder de menselijke beoordeling te vervangen; of (4) het voert een voorbereidende taak uit. Een systeem dat **profilering** uitvoert, wordt echter altijd geacht een significant risico op te leveren.

Elk in Annex III genoemd AI-systeem dat **profilering van natuurlijke personen** uitvoert, wordt automatisch als hoog risico beschouwd, ongeacht andere criteria. Onder **artikel 7** is de Commissie bevoegd Annex III via gedelegeerde handelingen te wijzigen — use-cases toevoegen, wijzigen of verwijderen. De Commissie moet jaarlijks beoordelen of wijziging nodig is.

> **Bottom line:** Classificatie is de spil van compliance. De Annex III-uitzondering biedt een legitieme uitweg voor procedurele of voorbereidende taken — maar vereist gedocumenteerde onderbouwing en registratie, en vervalt zodra er sprake is van profilering.

6. Verplichtingen voor hoog-risico AI-systemen (artikelen 9-15)

Hoog-risico AI-systemen mogen alleen in de Unie in de handel worden gebracht, in gebruik worden genomen of worden gebruikt als zij voldoen aan een set verplichte eisen. Deze eisen zijn **cumulatief** en gelden gedurende de volledige levenscyclus.

Artikel	Eis	Kern van de verplichting
Art. 9	Risicomanagementsysteem	Continu, iteratief proces gedurende de hele levenscyclus om bekende en voorzienbare risico's te identificeren en te mitigeren; regelmatig herzien en bijwerken
Art. 10	Data en datagovernance	Trainings-, validatie- en testdatasets moeten relevant, voldoende representatief en zo veel mogelijk foutloos en volledig zijn, met passende statistische eigenschappen en aandacht voor het mitigeren van bias

Art. 11	Technische documentatie	Opstellen vóór het in de handel brengen; toont aan dat het systeem voldoet en biedt autoriteiten de nodige informatie voor conformiteitsbeoordeling; up-to-date houden
Art. 12	Registratie/logging	Systeem moet automatische registratie van gebeurtenissen (logs) mogelijk maken gedurende de levensduur, ter facilitering van monitoring en traceerbaarheid
Art. 13	Transparantie en informatie aan gebruikers	Vergezeld van beknopte, duidelijke gebruiksaanwijzing die gebruikers in staat stelt capaciteiten en beperkingen te begrijpen
Art. 14	Menselijk toezicht	Ontworpen zodat natuurlijke personen effectief toezicht kunnen houden om risico's te voorkomen of te minimaliseren
Art. 15	Accuraatheid, robuustheid en cyberbeveiliging	Passende niveaus gedurende de levenscyclus; veerkrachtig tegen fouten en tegen pogingen tot manipulatie

Risicomanagement (art. 9). Het risicomanagementsysteem is een continu, iteratief proces dat gepland en uitgevoerd wordt gedurende de volledige levenscyclus. Het moet risico's identificeren en mitigeren, inclusief risico's uit **redelijkerwijs voorzienbaar misbruik** en uit de interactie tussen het systeem en zijn omgeving. De aanbieder moet de gemaakte keuzes documenteren en verklaren.

Data en datagovernance (art. 10). Datasets voor training, validatie en testen moeten relevant, voldoende representatief en zo veel mogelijk foutloos en volledig zijn. Bijzondere aandacht gaat naar het mitigeren van bias die grondrechten negatief kan beïnvloeden of tot verboden discriminatie kan leiden. Om bias te detecteren en te corrigeren mogen aanbieders bij uitzondering ook bijzondere categorieën persoonsgegevens verwerken, met passende waarborgen.

Menselijk toezicht (art. 14). De systemen moeten zo ontworpen zijn dat natuurlijke personen effectief toezicht kunnen houden. Passende maatregelen moeten waarborgen dat het systeem onderworpen is aan ingebouwde operationele beperkingen die het systeem zelf niet kan overschrijven. Voor bepaalde biometrische identificatiesystemen geldt een **verscherpte eis**: geen actie of beslissing mag worden genomen tenzij deze afzonderlijk is geverifieerd en bevestigd door ten minste **twee natuurlijke personen**.

Accuraatheid, robuustheid en cyberbeveiliging (art. 15). Technische robuustheid vereist veerkracht tegen fouten, storingen en onverwachte situaties, bijvoorbeeld via fail-safe-plannen. Cyberbeveiliging moet weerbaarheid bieden tegen AI-specifieke aanvallen zoals **data poisoning** (aanvallen op trainingsdatasets) en **adversarial attacks** of membership inference (aanvallen op getrainde modellen).

> **Bottom line:** Art. 9-15 vormen samen één geïntegreerd nalevingssysteem. Een compliance-programma dat slechts enkele artikelen adresseert, voldoet niet; de eisen zijn cumulatief en levenscyclusbreed. Datagovernance (art. 10) en menselijk toezicht (art. 14) zijn in de praktijk vaak de zwaarste posten.

7. Verplichtingen langs de waardeketen: aanbieders, gebruikers, importeurs, distributeurs

De verordening legt verplichtingen op aan alle schakels van de AI-waardeketen: aanbieders (providers), gebruikers (deployers), importeurs en distributeurs. De zwaarste verantwoordelijkheden rusten op de **aanbieder** — de entiteit die een AI-systeem ontwikkelt of laat ontwikkelen en op de markt brengt. De verordening voorziet echter ook in mechanismen voor **hercategorisering**: een gebruiker of importeur die een AI-systeem buiten het beoogde doel gebruikt, of die er een eigen naam of merk op plaatst, wordt juridisch behandeld als aanbieder met de bijbehorende zwaardere verplichtingen.

De **aanbieder** moet onder meer: het hoog-risico-systeem bouwen conform de vereisten van art. 9-15; een kwaliteitsmanagementsysteem opzetten en onderhouden; de EU-conformiteitsverklaring opstellen en de CE-markering aanbrengen; het systeem registreren in de EU-database; post-market monitoring uitvoeren; ernstige incidenten en gebreken melden; en correctieve maatregelen treffen. De **gebruiker (deployer)** draagt lichter maar niet triviaal: hij moet het systeem overeenkomstig de gebruiksaanwijzing gebruiken, zorgen dat de invoerdata relevant en representatief is, menselijk toezicht waarborgen conform art. 14, en ernstige incidenten melden. Gebruikers die **publieke autoriteiten** zijn of die hoog-risico-systemen inzetten die werknemers of kwestbare groepen beïnvloeden, hebben aanvullende informatieverstrekking en transparantieverplichtingen.

De verordening legt ook verplichtingen op aan **importeurs** (die controleren of aanbieders hun verplichtingen zijn nagekomen vóór het op de EU-markt brengen) en **distributeurs** (die controleren of de CE-markering aanwezig is en of de documentatie beschikbaar is in de vereiste taal). Zij mogen geen systemen op de markt brengen waarvan zij reden hebben om aan te nemen dat ze niet conform zijn.

Een kritiek mechanisme is de **waardeketen-cascade**: aanbieders van GPAI-modellen die aan downstream-aanbieders van hoog-risico-systemen leveren, moeten de noodzakelijke informatie en technische documentatie beschikbaar stellen zodat downstream-aanbieders hun eigen verplichtingen kunnen nakomen. Contractuele afspraken over de distributie van verantwoordelijkheid in de keten zijn daarmee een compliance-noodzaak, geen optie.

> **Bottom line:** Geen schakel in de waardeketen is vrij van verplichtingen. De juridische definitie van "aanbieder" is ruim genoeg om ook downstream-operators te omvatten die buiten het beoogde doel gebruiken of die een eigen merk aanbrengen. Keten-governance en contractuele allocatie van verantwoordelijkheden zijn essentieel.

8. AI-modellen voor algemene doeleinden (GPAI) en systeemrisico

De AI Act introduceert een apart regime voor **AI-modellen voor algemene doeleinden (General Purpose AI, GPAI)** — modellen die zijn getraind op brede data en die kunnen worden ingezet voor een groot aantal uiteenlopende taken. Dit omvat modellen die ten grondslag liggen aan generatieve AI-toepassingen. Het GPAI-regime is tweeledig:

- **Basisverplichtingen voor alle GPAI-aanbieders:** opstellen en bijhouden van technische documentatie; beschikbaar stellen van informatie en documentatie aan downstream-aanbieders die het model in hun producten integreren; naleving van auteursrechtregels (inclusief opt-outmechanismen voor webscrapers); en publicatie van een samenvatting van de gebruikte trainingsdata die voldoende gedetailleerd is om downstream-aanbieders in staat te stellen hun compliance te beoordelen.
- **Aanvullende verplichtingen voor modellen met systeemrisico:** modellen waarvan de cumulatieve hoeveelheid rekenkracht (floating point operations, FLOP) die is gebruikt voor training een bepaalde drempel overschrijdt — momenteel gesteld op 10^{25} FLOP — worden vermoed systeemrisico te hebben. Aanvullende verplichtingen omvatten: het uitvoeren van model-evaluaties (red teaming) conform gestandaardiseerde protocollen; het beoordelen en mitigeren van systeemrisico's inclusief hun bronnen; het melden van ernstige incidenten en correctieve maatregelen aan de Commissie; het waarborgen van passend niveau van cyberbeveiliging.

De FLOP-drempel voor systeemrisico is niet statisch: de verordening geeft de Commissie de bevoegdheid om de drempel bij gedelegeerde handeling aan te passen naarmate de technologie evolueert. Aanbieders van modellen die de drempel naderen, moeten de Commissie proactief informeren. Het **AI Office** is primair verantwoordelijk voor het toezicht op GPAI-aanbieders en kan bij overtreding sancties opleggen.

Een cruciaal onderscheid: aanbieders van GPAI-modellen die hun modellen als **open source** vrijgeven, zijn (met uitzondering van modellen met systeemrisico) vrijgesteld van de documentatieverplichtingen richting downstream-aanbieders. Modellen met systeemrisico die als open source worden vrijgegeven, blijven onderhevig aan de systeemrisico-verplichtingen, maar komen in aanmerking voor lichtere documentatievereisten als de aanbieder de gewichten beschikbaar stelt.

> **Bottom line:** Het GPAI-regime is een eigen nalevingscategorie die niet samenvalt met hoog-risico. Aanbieders van grote taalmodellen, multimodale modellen en andere brede modellen moeten zelfstandig beoordelen of zij als GPAI-aanbieder kwalificeren en of de systeemrisico-drempel wordt gehaald — ongeacht of hun downstream-gebruikers hoog-risico-toepassingen bouwen.

9. Transparantieverplichtingen

Naast de zware eisen voor hoog-risico-systemen en de specifieke GPAI-verplichtingen kent de verordening een lichtere maar brede laag van **transparantieverplichtingen** die gelden voor specifieke categorieën AI-systemen, ongeacht of zij als hoog-risico zijn geclassificeerd.

De voornaamste transparantieverplichtingen zijn:

- **Menselijke interactie.** AI-systemen die zijn ontworpen om met mensen te interacteren, moeten die personen informeren dat zij met een AI-systeem communiceren — tenzij dit uit de context duidelijk is voor een redelijk geïnformeerde gebruiker.

- **Deepfakes en synthetische content.** AI-systemen die beeld, audio, video of tekst genereren die echte mensen, plaatsen of gebeurtenissen nabootsen (deepfakes), moeten het kunstmatige karakter ervan duidelijk vermelden. Dit geldt ook voor generatieve AI-systemen die tekst produceren over zaken van publiek belang.
- **Emotieherkenning en biometrische categorisering.** Gebruikers van emotieherkenningssystemen en biometrische categorisatiesystemen die niet zijn verboden, moeten de betrokkenen informeren over het gebruik van dergelijke systemen.
- **Content provenance.** Aanbieders van GPAI-systemen die synthetische content genereren, moeten zorgen voor machine-readable markering (zoals watermarking) zodat de kunstmatige herkomst kan worden geverifieerd — ook door geautomatiseerde systemen.

De transparantieverplichtingen zijn minder zwaar dan de hoog-risico-eisen, maar zijn juridisch afdwingbaar en raken alle actoren die chatbots, AI-writers, deepfake-tools of emotieanalyse inzetten, ongeacht risicoklasse.

> **Bottom line:** Transparantie is de derde laag van de verordening — breed van reikwijdte en van toepassing op systemen die anders als "minimaal risico" worden beschouwd. Elke organisatie die klantgerichte AI-tools inzet, moet de transparantieverplichtingen toetsen, ook als hoog-risico-classificatie niet aan de orde is.

10. Conformiteitsbeoordeling en post-market monitoring

Voordat een hoog-risico AI-systeem op de EU-markt wordt gebracht of in gebruik wordt genomen, moet een **conformiteitsbeoordeling** worden uitgevoerd. De wijze waarop verschilt naargelang de route waarop het systeem als hoog-risico is geclassificeerd:

- **Annex I-systemen (geïntegreerd in gereguleerde producten):** de conformiteitsbeoordeling verloopt conform de sectorale wetgeving (bijv. de MDR voor medische hulpmiddelen, de Machinery Directive voor machines). De AI-specifieke vereisten worden meegenomen in de bestaande beoordelingsprocedure, doorgaans uitgevoerd door een aangemelde instantie (notified body).
- **Annex III-systemen (stand-alone):** voor de meeste stand-alone hoog-risico-systemen mag de aanbieder een **interne conformiteitsbeoordeling** uitvoeren — een zelfevaluatie aan de hand van de vereisten van art. 9-15. Uitzondering: voor AI-systemen voor biometrische identificatie op afstand in openbare ruimten voor rechtshandhaving (die niet verboden zijn) is een conformiteitsbeoordeling door een derde instantie vereist.

Na de conformiteitsbeoordeling stelt de aanbieder de **EU-conformiteitsverklaring** op en brengt de **CE-markering** aan. Het systeem wordt vervolgens geregistreerd in de **EU-database voor hoog-risico AI-systemen**. Deze database is openbaar toegankelijk en bevat basisinformatie over elk geregistreerd systeem; voor rechtshandhaving- en migratie-systemen geldt een beperkte toegang.

Post-market monitoring is een doorlopende verplichting. Aanbieders moeten een post-market monitoringsysteem opzetten dat actief informatie verzamelt en analyseert over de prestaties van het systeem gedurende zijn levensduur. Bij ontdekking van ernstige incidenten of niet-conform gedrag moet de aanbieder de

bevoegde nationale autoriteit informeren en, zo nodig, het systeem uit de handel nemen of aanpassen. Gebruikers spelen hierin ook een rol: zij zijn verplicht ernstige incidenten en functionele storingen te melden aan de aanbieder of importeur.

> **Bottom line:** Conformiteitsbeoordeling is geen eenmalig certificeringsmoment maar het begin van een doorlopende nalevingscyclus. Post-market monitoring en incidentmelding vereisen operationele processen die al vóór ingebruikname moeten zijn ingericht.

11. Governance en toezichthoudende instanties

De AI Act creëert een meerlaagsgovernancestructuur met zowel EU-niveau als nationale componenten:

- **AI Office (Europese Commissie).** Het AI Office is opgericht binnen de Europese Commissie en fungeert als primaire Unie-level toezichthouder. Het is verantwoordelijk voor het toezicht op GPAI-aanbieders, het bevorderen van uniforme toepassing van de verordening, het ondersteunen van nationale autoriteiten, het beheren van het EU-brede meldingssysteem voor incidenten, en het uitvoeren van onderzoeken naar aanbieders van GPAI-modellen met systeemrisico. Het AI Office heeft de bevoegdheid om sancties op te leggen aan GPAI-aanbieders.
- **European Artificial Intelligence Board (AI Board).** De AI Board is samengesteld uit vertegenwoordigers van de nationale markttoezichtautoriteiten en de Europese Toezichthouder voor gegevensbescherming. De Board adviseert en ondersteunt de Commissie bij de uitvoering van de verordening, bevordert samenwerking tussen nationale autoriteiten, en geeft adviezen over de interpretatie en toepassing van de verordening.
- **Wetenschappelijk panel van onafhankelijke deskundigen.** De Commissie stelt een wetenschappelijk panel in van maximaal 60 onafhankelijke deskundigen dat het AI Office en de AI Board bijstaat bij technische vraagstukken, met name bij de beoordeling van GPAI-modellen met systeemrisico en bij het adviseren over het bijwerken van de annexen.
- **Nationale markttoezichtautoriteiten.** Elke lidstaat wijst een of meer nationale autoriteiten aan die verantwoordelijk zijn voor het toezicht op de toepassing van de verordening op hun grondgebied, met name voor hoog-risico AI-systemen. Deze autoriteiten hebben bevoegdheden om inspecties uit te voeren, documenten op te vragen en, bij overtreding, sancties op te leggen.

De verordening voorziet ook in een **adviesforum** — een breed samengesteld forum met vertegenwoordigers van het bedrijfsleven, de academische wereld, het maatschappelijk middenveld en nationale autoriteiten — dat de Commissie en de AI Board van informatie voorziet over de uitvoering van de verordening.

> **Bottom line:** De governance is bewust gelaagd om zowel consistentie op EU-niveau als nationale uitvoering te waarborgen. Organisaties moeten weten welke nationale autoriteit hun bevoegde toezichthouder is en moeten relaties onderhouden met zowel nationale als EU-niveau instanties, afhankelijk van hun activiteiten.

12. Meldplicht bij ernstige incidenten en sancties

De verordening legt een **meldplicht bij ernstige incidenten** op. Een "ernstig incident" is een incident of een gebrek dat direct of indirect leidt of kan leiden tot overlijden of ernstig letsel, schade aan infrastructuur, goederen of het milieu, of significante schade aan grondrechten. Aanbieders van hoog-risico AI-systemen die al op de markt zijn, zijn verplicht ernstige incidenten onverwijld te melden aan de nationale markttoezichtautoriteiten van de lidstaten waar het incident heeft plaatsgevonden.

De **sancties onder artikel 99** zijn ontworpen om doeltreffend, evenredig en afschrikkend te zijn:

- Overtreding van verboden uit artikel 5 (verboden AI-praktijken): maximaal **35 miljoen euro** of, voor ondernemingen, **7% van de wereldwijde jaarlijkse omzet** (het hoogste van de twee).
- Overtreding van andere verplichtingen voor hoog-risico AI-systemen: maximaal **15 miljoen euro** of **3% van de wereldwijde jaarlijkse omzet**.
- Het verstrekken van onjuiste, onvolledige of misleidende informatie aan bevoegde autoriteiten: maximaal **7,5 miljoen euro** of **1% van de wereldwijde jaarlijkse omzet**.
- Voor kleine en middelgrote ondernemingen (kmo's) en startups gelden lagere boeteplafonds — het lagere van de twee bedragen is leidend.

Naast financiële sancties kunnen bevoegde autoriteiten ook bevelen om systemen uit de handel te nemen, de toegang ertoe te beperken of het gebruik ervan op te schorten. De Commissie heeft voor GPAI-aanbieders met systeemrisico aanvullende handhavingsbevoegdheden, waaronder periodieke boetes.

> **Bottom line:** Het sanctiekader is vergelijkbaar met dat van de AVG — hoge plafonds, omzetgerelateerd, met differentiatie voor kmo's. Een incident-response- en meldproces moet vóór ingebruikname operationeel zijn. Preventie is economisch rationeel: de kosten van compliance zijn vrijwel zeker lager dan de kosten van overtreding.

13. Tijdlijn, inwerkingtreding en toepassingsdata

De AI Act is gefaseerd van kracht geworden. De sleutelmijlpalen zijn:

Datum	Wat wordt van kracht
1 augustus 2024	Inwerkingtreding van de verordening (publicatie + 20 dagen)
2 februari 2025	Verboden AI-praktijken (art. 5) van toepassing; definitiehoofdstuk van toepassing
2 augustus 2025	GPAI-verplichtingen van toepassing; governance en toezichtsstructuur operationeel; gedragscodes voor GPAI verwacht

2 augustus 2026	Meeste hoog-risico-verplichtingen (art. 9-15, conformiteitsbeoordeling, registratie) van toepassing; transparantieverplichtingen van toepassing; post-market monitoring van toepassing
2 augustus 2027	Volledig kader van toepassing, inclusief Annex I-systemen (in gereguleerde producten); uitgestelde toepassing voor bepaalde hoog-risico-categorieën indien afhankelijk van nog te ontwikkelen geharmoniseerde standaarden

Bestaande hoog-risico AI-systemen die al vóór augustus 2026 in gebruik zijn en niet significant zijn gewijzigd, kunnen in aanmerking komen voor verlengde overgangsperiodes. De exacte overgangsbepalingen zijn afhankelijk van de categorie en het gebruik van het systeem.

De verordening voorziet ook in **gedelegeerde en uitvoeringshandelingen** die de Commissie bevoegd is vast te stellen om de bijlagen te wijzigen, geharmoniseerde normen te verwijzen en specificaties te preciseren. De tijdlijn voor deze gedelegeerde handelingen is niet volledig bepaald en wordt nader ingevuld naarmate de markt en technologie zich ontwikkelen.

> **Bottom line:** De tijdlijn loopt nu al. Compliance-roadmaps moeten aan de kalender worden verankerd. Het meest urgente: verboden toepassingen beoordelen (al van kracht), GPAI-positie bepalen (van kracht augustus 2025), en hoog-risico-systemen documenteren en voorbereiden voor augustus 2026.

14. Bijlagen (annexen)

De verordening bevat meerdere technische bijlagen die cruciaal zijn voor de praktische toepassing:

- **Annex I — Unieharmonisatiewetgeving.** De lijst van sectorale wetgeving waaronder AI-systemen als hoog-risico kwalificeren via de Annex I-route. Omvat onder meer richtlijnen en verordeningen voor machines, speelgoed, medische hulpmiddelen, voertuigen en luchtvaart. De Commissie kan deze lijst bijwerken via gedelegeerde handelingen.
- **Annex II — Lijst van Uniehorizontale wetgeving inzake databescherming.** Relevante wetgeving voor de toepassing van de AI Act in samenhang met databeschermingsregels.
- **Annex III — Hoog-risico AI-systemen (stand-alone).** De acht domeinen en de bijbehorende use-cases die als hoog risico worden geclassificeerd. Dit is de meest operationeel relevante bijlage voor de meeste organisaties. De bijlage kan door de Commissie worden bijgewerkt; jaarlijkse herziening is verplicht.
- **Annex IV — Technische documentatie voor hoog-risico AI-systemen.** De minimumeisen voor de technische documentatie die aanbieders van hoog-risico-systemen moeten opstellen en bijhouden. Omvat beschrijving van het systeem, de data en het trainingsproces, de risicobeoordeling en de conformiteitsbeoordeling.
- **Annex V — EU-conformiteitsverklaring.** De vereiste inhoud van de conformiteitsverklaring die de aanbieder opstelt voor hoog-risico AI-systemen.
- **Annex VI en VII — Conformiteitsbeoordelingsprocedures.** Procedure A (interne beoordeling) voor de meeste Annex III-systemen; Procedure B (derde-partijbeoordeling) voor specifieke systemen, met name biometrische identificatiesystemen voor rechtshandhaving.

- **Annex VIII, IX, X — GPAI-documentatie en registratie.** Vereisten voor technische documentatie van GPAI-modellen (inclusief modellen met systeemrisico), informatie-eisen voor downstream-aanbieders, en registratieverplichtingen.

> **Bottom line:** De annexen zijn geen bijkomende details — zij zijn het operationele hart van de verordening. Annex III bepaalt wie als hoog risico kwalificeert; Annex IV bepaalt wat moet worden gedocumenteerd; Annex VIII bepaalt wat GPAI-aanbieders moeten bijhouden. Elke compliance-implementatie moet bij de relevante annexen beginnen.

15. Beslissingskader: hoe classificeert en prioriteert u?

Gegeven de breedte en complexiteit van de verordening, biedt onderstaand beslissingskader een praktische navigatiestructuur voor compliance-besluitvormers.

Stap 1: Val ik onder de verordening?
Beoordeel of uw organisatie kwalificeert als aanbieder, gebruiker, importeur of distributeur van AI-systemen waarvan de output in de EU wordt gebruikt. Zo ja: de verordening is van toepassing, ongeacht uw vestigingsplaats.

Stap 2: Gebruik ik verboden AI-praktijken?
Scan uw AI-portfolio op de zeven verbodscategorieën van art. 5. Dit is de meest urgent te adresseren vraag, want verboden zijn sinds 2 februari 2025 afdwingbaar. Betrek juridische expertise bij twijfelgevallen.

Stap 3: Ben ik GPAI-aanbieder?
Als uw organisatie een AI-model ontwikkelt of aanbiedt dat voor een breed scala van taken kan worden ingezet, kwalificeert u waarschijnlijk als GPAI-aanbieder. Verplichtingen zijn van toepassing vanaf augustus 2025. Beoordeel of de systeemrisico-drempel (10^{25} FLOP) wordt gehaald of benaderd.

Stap 4: Heb ik hoog-risico AI-systemen?
Toets elk AI-systeem in uw portfolio aan Annex I (gereguleerde producten) en Annex III (acht domeinen). Documenteer de classificatiebeslissing, inclusief eventuele toepassing van de Annex III-uitzondering.

Stap 5: Bouw het compliance-programma op.
Voor hoog-risico-systemen: implementeer art. 9-15 als geïntegreerd programma (niet als losse maatregelen). Zet een kwaliteitsmanagementsysteem op, stel de technische documentatie op, richt logging en monitoring in, en bereid de conformiteitsbeoordeling voor. Zorg voor operationele incidentmelding- en post-market monitoringprocessen vóór ingebruikname.

Stap 6: Veranker in de waardeketen.
Sluit contractuele afspraken met upstream-aanbieders (GPAI-leveranciers, component-aanbieders) en downstream-gebruikers over de verdeling van compliance-verantwoordelijkheden. Zorg dat contracten de vereiste informatiestroom (technische documentatie, incidentmelding) faciliteren.

> **Bottom line:** Compliance begint bij classificatie en eindigt bij monitoring. Het beslissingskader is sequentieel: verboden eerst, GPAI daarna, hoog-risico vervolgens, transparantie breed. Geen stap overslaan. Documenteer elke

> beslissing — de bewijslast ligt bij de organisatie, niet bij de toezichthouder.

Aanbevelingen

Op basis van de analyse van Verordening (EU) 2024/1689 worden de volgende aanbevelingen geformuleerd voor organisaties die AI-systemen ontwikkelen, aanbieden of gebruiken in of gericht op de Europese Unie:

1. Start met een AI-inventarisatie en classificatie

Breng alle AI-systemen in kaart die uw organisatie ontwikkelt, aanbiedt of gebruikt. Classificeer elk systeem conform de risicogebaseerde benadering van de AI Act: verboden, hoog risico, transparantieverplichting, of minimaal risico. Documenteer de classificatiebeslissing, inclusief de gebruikte criteria en eventuele toepassing van de Annex III-uitzondering. Herhaal deze inventarisatie periodiek, gezien de mogelijkheid van wijziging van Annex III.

2. Implementeer een compliance-roadmap op basis van de gefaseerde tijdlijn

De meest urgente stap was het verwijderen van verboden praktijken (afdwingbaar per 2 februari 2025). Daarna volgt GPAI-compliance (augustus 2025) en vervolgens hoog-risico-compliance (augustus 2026). Ontwikkel een roadmap die aan deze kalender is verankerd en die voldoende ruimte laat voor implementatie, testing en documentatie van elk verplichtingspakket.

3. Behandel het hoog-risico-pakket als geïntegreerd kwaliteitssysteem

De vereisten van art. 9-15 zijn ontworpen als samenhangend systeem, niet als losstaande maatregelen. Implementeer risicomanagement (art. 9), datagovernance (art. 10), technische documentatie (art. 11), logging (art. 12), transparantie (art. 13), menselijk toezicht (art. 14) en technische kwaliteit (art. 15) als onderdelen van één geïntegreerd kwaliteitsmanagementsysteem. Verankerd in bestaande ISO- of sectorspecifieke kwaliteitsstandaarden waar mogelijk.

4. Richt post-market monitoring en incidentmelding in voor ingebruikname

De meldplicht bij ernstige incidenten en de post-market monitoringverplichting zijn doorlopend en beginnen bij ingebruikname — niet pas daarna. Richt de benodigde processen, verantwoordelijkheden en technische infrastructuur in vóór de lancering van een hoog-risico-systeem. Zorg dat medewerkers weten wat een "ernstig incident" is en hoe het gemeld moet worden.

5. Beoordeel de GPAI-positie proactief

Als uw organisatie grote taalmodellen, multimodale modellen of andere brede AI-modellen ontwikkelt of aanbiedt, beoordeel dan proactief of u als GPAI-aanbieder kwalificeert en of de systeemrisico-drempel relevant is. Stel de vereiste technische documentatie en trainingsdata-samenvatting op. Informeer de Commissie als u de systeemrisico-drempel benadert of overschrijdt.

6. Veranker compliance in de contractuele keten

AI-compliance is geen solo-activiteit. Sluit contracten met upstream-leveranciers (GPAI-modellen, data, componenten) die de vereiste informatiestroom (technische documentatie, trainingsdata-samenvatting, incidentmelding) garanderen. Maak afspraken met downstream-gebruikers over hun verplichtingen als deployer. Zorg dat contracten voorzien in hercategorisering als gebruiker als aanbieder optreedt.

7. Investeer in AI-geletterdheid en governancecapaciteit

De AI Act veronderstelt een minimum aan AI-geletterdheid bij zowel aanbieders als gebruikers. Investeer in opleiding van medewerkers die AI-systemen ontwikkelen, inzetten of toezicht houden — met name op het gebied van risicobeoordeling, datagovernance en menselijk toezicht. Overweeg de aanstelling van een AI-compliance-officer of de uitbreiding van bestaande compliance- en DPO-functies.

8. Volg de voortschrijdende regelgeving actief

De AI Act is een levend kader: Annex III wordt jaarlijks herzien, gedelegeerde handelingen worden verwacht, de Digital Omnibus on AI-vereenvoudigingen zijn in behandeling, en geharmoniseerde standaarden zijn nog in ontwikkeling. Stel een monitoringproces in voor EU-regelgeving en pas compliance-programma's tijdig aan. Deelname aan openbare consultaties en brancheorganisaties biedt vroegtijdige signalering van wijzigingen.

Kanttekeningen en Beperkingen

Dit document is opgesteld als interne naslagreferentie op basis van de officiële EUR-Lex/Publicatieblad-tekst van Verordening (EU) 2024/1689. Bij de interpretatie en het gebruik ervan gelden de volgende kanttekeningen:

Overwegingen versus artikelen

Een groot deel van de gedetailleerde formuleringen in dit document is afkomstig uit de **overwegingen (recitals)** van de verordening. Overwegingen geven de bedoeling en context weer maar zijn juridisch niet op dezelfde wijze bindend als de artikelen. Waar dit rapport artikelinhoud beschrijft (bijv. art. 9-15, 73, 99), is dat deels gebaseerd op officiële samenvattingen van de artikelen; de exacte, volledige artikeltekst moet in de authentieke versie worden gecontroleerd.

Bijlagen

De volledige, woordelijke inhoud van de bijlagen (met name de gedetailleerde lijsten in Annex I en Annex III en de technische bijlagen voor GPAI) was niet integraal in de brondata beschikbaar. De in dit rapport opgenomen samenvatting van de bijlagen is afgeleid uit de overwegingen en officiële beschrijvingen.

Toekomstgerichte en in beweging zijnde elementen

De **Digital Omnibus on AI (COM/2025/836)** is een **voorstel** van november 2025 en geen vastgesteld recht; de beschreven vereenvoudigingen kunnen wijzigen of niet worden aangenomen. Ook de compute-drempel voor systeemrisico is bedoeld om over de tijd te worden aangepast. Data en governance-details zijn afkomstig uit officiële EU-communicatie en kunnen in de loop van de tijd wijzigen.

Geen juridisch advies

Dit document is bedoeld voor intern gebruik als naslagwerk en vormt **geen juridisch advies**. Voor concrete compliance-beslissingen dient de authentieke wettekst en, waar nodig, gespecialiseerd juridisch advies te worden geraadpleegd.

> **Slotsom:** Gebruik dit document als navigatie- en prioriteringsinstrument bovenop — niet in plaats van — de authentieke tekst op EUR-Lex. De kern van AI Act-compliance is stabiel en afdwingbaar; de randen (Omnibus, standaarden, gedelegeerde handelingen) blijven in beweging en vergen periodieke herziening.

Bronvermelding

Dit document is samengesteld op basis van de volgende officiële EU-bronnen. Alle bronnen zijn openbaar beschikbaar via EUR-Lex of de websites van de relevante EU-instellingen.

[1] Verordening (EU) 2024/1689 van het Europees Parlement en de Raad — officiële tekst (EUR-Lex): https://eur-lex.europa.eu/eli/reg/2024/1689/oj

[2] Europese Commissie — evaluatieverslag AI Act (COM/2025/723): https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52025DC0723

[3] Publicatieblad van de EU — volledige PDF-versie Verordening 2024/1689: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401689

[4] EUR-Lex — officiële samenvatting (Legal Summary Unit): https://eur-lex.europa.eu/legal-content/EN/LSU/?uri=oj:L_202401689

[5] Europese Commissie — Digital Omnibus on AI voorstel (COM/2025/836): https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025PC0836

[6] Comité van de Regio's — advies inzake territoriale impact AI Act: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021AR2682

[7] Volledig PDF-bestand Verordening 2024/1689 (geconsolideerde versie): https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32024R1689&from=EN

[8] HTML-versie Publicatieblad — Verordening 2024/1689: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ%3AL_202401689

[9] Digital Omnibus voorstel (vereenvoudigingen hoog-risico): https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52025PC0836

[10] Commissie analyse implementatievereenvoudiging AI Act: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52025PC0836

[11] Commissie evaluatierapport Annex III herziening (COM/2026/234): https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A52026DC0234

[12] EUR-Lex officiële samenvatting — regels voor betrouwbare AI: https://eur-lex.europa.eu/EN/legal-content/summary/rules-for-trustworthy-artificial-intelligence-in-the-eu.html

[13] European AI Office — officiële website: https://digital-strategy.ec.europa.eu/en/policies/ai-office

[14] European Artificial Intelligence Board — officiële pagina: https://digital-strategy.ec.europa.eu/en/policies/ai-board

[15] Uitvoeringsverordening (EU) 2025/454 — AI Board procedures: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32025R0454

[16] Geconsolideerde tekst Verordening 2024/1689: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689

[17] Origineel Commissievoorstel COM/2021/206: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A52021PC0206

[18] HTML toelichting Digital Omnibus vereenvoudigingen: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52025PC0836

[19] Europees Parlement resolutie over AI Act interpretatie: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52025IP0286

[20-34] Overige EUR-Lex bronnen — volledige lijst beschikbaar via: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng

---

Samengesteld door **The AI Content Engineer** | Verordening (EU) 2024/1689 | Publicatie 2024

Dit document vormt geen juridisch advies. Raadpleeg voor concrete compliance-beslissingen de authentieke wettekst en gespecialiseerde juridische expertise.