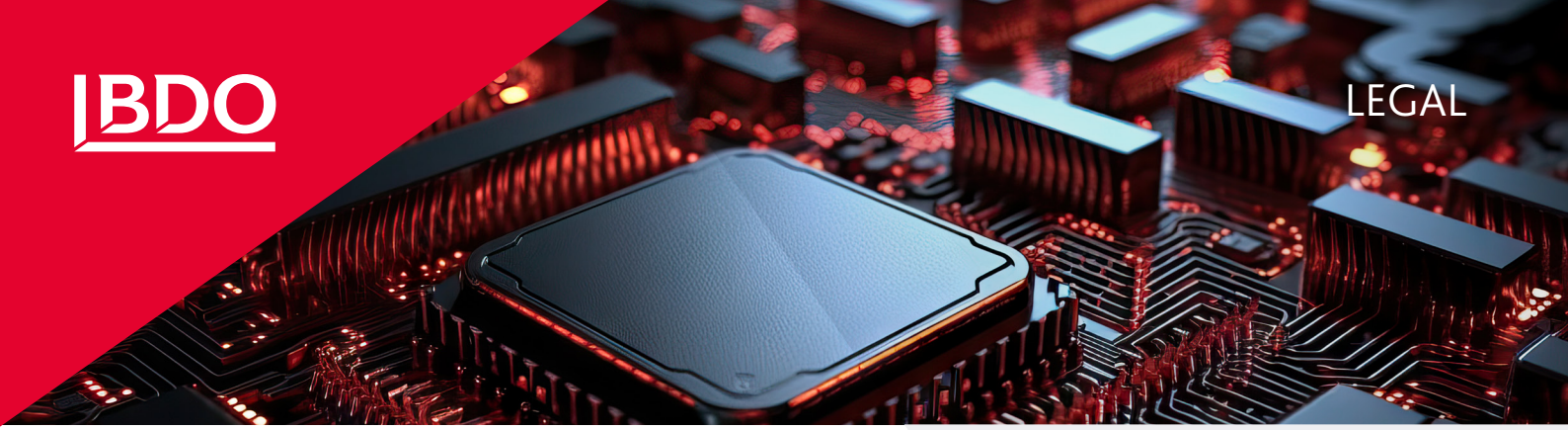

LEGAL

Update Europese techregulering

De Europese Unie (EU) heeft zich de afgelopen jaren sterk ingezet op het moderniseren en harmoniseren van wetgeving rondom digitale technologie, data en kunstmatige intelligentie. Deze ontwikkelingen hebben niet alleen invloed op technologiebedrijven, maar raken alle organisaties en eindgebruikers die werken met digitale systemen, platforms of AI-oplossingen. Hieronder volgt een overzicht van vier belangrijke wetgevingstrajecten: de AI Act, NIS2, Digital Services Act (DSA) en Digital Markets Act (DMA), inclusief de praktische en juridische consequenties voor gebruikers.

AI Act

De AI Act is het eerste uitgebreide Europese wetgevingskader dat specifiek gericht is op kunstmatige intelligentie (ook wel artificial intelligence, AI). Deze verordening, die in augustus 2027 in werking treedt, heeft als doel innovatie te stimuleren, risico's te beteugelen en het vertrouwen in AI te bevorderen, zodat de rechten van individuen worden gewaarborgd. Bepaalde verplichtingen zijn nu al van kracht of treden op korte termijn in werking. Organisaties doen er dus goed aan om op dit moment daar al op voor te sorteren.
De AI Act is van toepassing op een breed scala aan organisaties binnen de Europese Unie. Dit zijn:

- Ontwikkelaars van AI-systemen (zowel bedrijven als onderzoeksinstellingen);
- Leveranciers en distributeurs van AI-oplossingen;
- Importeurs die AI-systemen van buiten de EU op de Europese markt brengen; én
- Gebruikers van AI-systemen (zoals bedrijven die AI inzetten voor of in hun processen of producten).

Let daarbij dus op! Ook wanneer uw organisatie AI inzet van een leverancier (en deze dus niet zelf ontwikkelt), zullen daarbij verplichtingen uit de AI Act gelden.

De AI Act kent een risico gebaseerde aanpak waarbij kortgezegd geldt: hoe hoger het risico van het AI-systeem, hoe strenger de eisen waaraan deze moet voldoen.

De AI Act classificeert deze zoals onderstaand:

- ***Verboden AI:*** AI-toepassingen die fundamentele rechten schaden, zoals social scoring of emotieherkenning op het werk en/of in het onderwijs, zijn verboden. Dit verbod geldt sinds februari 2025.
- ***Hoog-risico AI:*** Bijvoorbeeld AI voor biometrische identificatie, recruitment, of de toelating van studenten in het onderwijs. Voor deze systemen gelden strenge eisen op het gebied van transparantie, risicobeheer, menselijke controle en cybersecurity. Voor gebruikers daarvan betekent onder meer dat zij:
  - (i) Verplicht informatie over het systeem, de werking en de beperkingen moeten geven.
  - (ii) Training moeten faciliteren voor medewerkers die met deze systemen werken.
  - (iii) Actief monitoren van de werking en het rapporteren van incidenten of bijwerkingen.
- ***Beperkt risico:*** Bijvoorbeeld chatbots. Hierbij geldt onder andere dat gebruikers altijd moeten worden geïnformeerd dat zij met een AI-systeem communiceren.

Voor alle bovengenoemde categorieën geldt dat transparantie, verantwoordelijkheid, juist gebruik van persoonsgegevens volgens de Algemene Verordening Gegevensbescherming (AVG) en ethische inzet centraal staan. Organisaties die AI gebruiken dienen hun processen, documentatie en training hierop in te richten. Niet-naleving kan leiden tot hoge boetes tot wel 15 miljoen euro of 3% van de jaaromzet, of aansprakelijkheid.

Hoewel deze verordening pas in augustus 2027 volledig in werking treedt, zijn een aantal verplichtingen al van kracht. Zo is op 2 februari 2025 het verbod op de verboden AI in de AI Act al van toepassing en moeten organisaties die AI-systemen ontwikkelen of gebruiken zorgen dat hun werknemers AI-geletterd zijn. Dat houdt in dat zij ervoor moeten zorgen dat het personeel over voldoende kennis en vaardigheden beschikt om AI op een verantwoorde manier in te zetten. In augustus 2025 zijn de bepalingen over general purpose AI-modellen in werking getreden en moet het toezicht daarop zijn ingericht. Dit zijn modellen die de basis vormen voor andere toepassingen, zoals de taalmodellen die worden gebruikt voor AI-chatbots.

Wat kunt u doen?

- Inventariseer welke AI toepassingen u gebruikt (zoals camera's, maar ook ChatGPT, Microcosft CoPilot, chatbots etc.)
- Classificeer in welke risicogroep deze vallen.
- Ga na of u gebruik maakt van (mogelijk) verboden AI praktijken of general purpose AI modellen en onderzoek of u voldoet aan de vereisten van deze modellen.
- Ga na of uw personeel AI-geletterd is, of dat zij meer opleiding nodig hebben.
- De AVG speelt zowel bij het trainen van AI (de gebruikte datasets) als bij de toepassing van AI (de verwerking van gegevens van eindgebruikers) een belangrijke rol. Compliance met de AVG moet bovendien aantoonbaar zijn.

NIS2 (Netwerk- en Informatiebeveiliging)

De NIS2 Richtlijn is bedoeld om cyberbeveiliging en weerbaarheid van essentiële diensten in de EU te verbeteren, door het voorschrijven van o.a. beveiligingsnormen en meldingsvereisten voor incidenten. Nederland had deze richtlijn al moeten implementeren, echter is de verwachting dat dit pas in 2026 plaats zal vinden. De NIS2 is van toepassing op een brede groep organisaties die een essentiële of belangrijke rol spelen in de economie en samenleving van de EU. Ten opzichte van de oorspronkelijke NIS-richtlijn is de scope van NIS2 aanzienlijk uitgebreid. NIS2 geldt onder meer voor:

- ***Essentiële entiteiten:*** organisaties in sectoren zoals energie, transport, bankwezen, gezondheidszorg, drinkwater, digitale infrastructuur, overheid en ruimtevaart.
- ***Belangrijke entiteiten:*** organisaties in bijvoorbeeld post- en koeriersdiensten, afvalwaterbeheer, voedselproductie, chemische industrie, producenten van medische hulpmiddelen, digitale aanbieders (zoals cloud computing, datacenters, online marktplaatsen), en aanbieders van beheerde IT-diensten.

De richtlijn is van toepassing op zowel grote als middelgrote bedrijven en organisaties die binnen deze sectoren in de Europese Unie actief zijn. Kleine bedrijven (minder dan 50 werknemers en/of minder dan €10 miljoen omzet per jaar) zijn in principe uitgezonderd, tenzij zij een cruciale rol spelen of diensten leveren waarvan uitval grote gevolgen kan hebben.

Niet-naleving kan leiden tot hoge boetes en reputatieschade. Een belangrijk onderdeel is dat de NIS2-richtlijn bestuurders aansprakelijk stelt voor het niet naleven van deze verplichtingen.

Wat kunt u doen?

Hoewel is aangegeven dat de implementatie van de NIS2-richtlijn is uitgesteld tot 2026, betekent dit niet dat u niet alvast stappen kunt nemen. Denk aan:

- Bepaal of u als een essentiële of belangrijke organisatie kwalificeert, of dat u daaraan levert.
- Bestuurders moeten opgeleid worden om risico's te kunnen identificeren en risicobeheerspraktijken te kunnen beoordelen;
- Een risicoanalyse en beleid inzake beveiliging van informatiesystemen opzetten;
- Incidentpreventie en -response voor uw organisatie opzetten;
- Beveiliging van de toeleveringsketen onderzoeken; én
- Beleid en procedures voor beheer van cyberbeveiligingsricico's opstellen.

Digital Services Act (DSA) en Digital Markets Act (DMA)

De Digital Services Act (DSA) en de Digital Markets Act (DMA) richten zich op online platformen. De DMA is vooral gericht op het vergroten van de verantwoordelijkheid van onlineplatforms voor de inhoud die erop wordt geplaatst. De DMA richt zich alleen op de grootste partijen, maar heeft in potentie wel positieve effecten op kleinere partijen. De DSA richt zich met name op het bevorderen van een transparante en veilige online omgeving voor een reeks aanbieders van digitale diensten.

De DSA richt zich op digitale diensten, zoals tussenhandelsdiensten die netwerkinfrastructuur aanbieden (internetproviders, domeinnaam-registrators), hostingdiensten (cloud- en webhostingdiensten), onlineplatforms zoals onlinemarktplaatsen, app-stores, deeleconomieplatforms en sociale media platforms en zoekmachines, die als bemiddelaars fungeren tussen gebruikers en content.

De DSA legt verplichtingen op met betrekking tot transparantie en omgang met inhoud (inclusief contentmoderatie en advertenties). Het meest strenge regime geldt voor zogenaamde 'gatekeepers'. Platforms met een groot gebruikersbereik en impact worden aangemerkt als 'gatekeepers' en moeten extra informatie verstrekken en toezicht houden op concurrentie-aspecten. De DSA is dus niet alleen van toepassing op de gatekeepers, maar ook op de kleinere partijen, waarvoor een milder regime geldt. Echter, indien het creëren van user generated content slechts een bijkomstig kenmerk is van de dienst op een online platform, is de DSA niet van toepassing. Daarentegen gelden er voor hostingdiensten juist extra verplichtingen.

Begin dit jaar heeft de Eerste Kamer ingestemd met de implementatiewetten voor de DSA en DMA en zijn deze in werking getreden. Dit houdt concreet in dat vanaf 4 februari 2025 de Autoriteit Consument & Markt (ACM) officieel

bevoegd is om toezicht te houden op de naleving van de DSA. Indien iemand van mening is dat een aanbieder van een online platform of dienst zich niet houdt aan de DSA, kunnen zij dit melden bij de ACM, waarna deze kan handhaven. Daarnaast is ook de Autoriteit Persoonsgegevens een bevoegde autoriteit, deze houdt toezicht op profilering bij het tonen van reclames op online platforms. Voor gevallen onder de DMA geldt dat deze nationale autoriteiten een ondersteunende rol heeft, maar dat de Europese Commissie zal handhaven.

Wat kunt u doen?

- Vaststellen onder welke categorie, en dus welk regime, van de DSA u valt;
- Het aanpassen van uw algemene voorwaarden of gebruiksvoorwaarden, bijvoorbeeld door: informatie te geven over de inhoudsmoderatie, algoritmische besluitvorming en menselijke controle daarbij;
- Notice & takedown mechanismes inrichten (voor indienen en afhandelen van meldingen over illegale inhoud);
- Het opzetten van een klachtenafhandelingssysteem en omgang met illegale content (beperking zichtbaarheid, schorsing/beëindiging van accounts etc.);
- Het opzetten van een 'know your customer'-procedure;
- Het gemiddeld aantal actieve gebruikers over de afgelopen 6 maanden bijhouden indien vereist;
- Een contactpunt aanwijzen voor de overheid en afnemers;
- Beperkingen op het gebruik van de dienst uitleggen op een manier die minderjarigen kunnen begrijpen.

Let op: Voor grotere ondernemingen (vanaf 50 werknemers, omzet vanaf 12 miljoen of activa vanaf 6 miljoen) en zeer grote platformen (maandelijks 45 miljoen afnemers of meer), gelden veel extra verplichtingen.

Conclusie

De hiervoor beschreven reguleringen zorgen voor veel (aankomende) veranderingen. De technologische ontwikkelingen gaan daarnaast ook snel. Zowel organisaties als individuele gebruikers profiteren van betere bescherming en meer rechten, maar dienen zich te realiseren dat ook hun eigen verantwoordelijkheid groeit. Voorbereiding, bewustwording en tijdige aanpassing aan deze regelgeving zijn essentieel om juridische en operationele risico's te vermijden en maximaal te profiteren van digitale innovatie. Daarnaast zijn de handhavingsmogelijkheden uitgebreid, waardoor het risico op boetes en/of bestuurdersaansprakelijkheid toeneemt.

MEER INFORMATIE

Hulp nodig om het bovenstaande in kaart te brengen voor uw eigen organisatie? Voor vragen of verdere toelichting kunt u contact opnemen met een van onderstaande contactpersonen.

Femke Schemkes
Jurist Tech & Privacy recht
E femke.schemkes@bdo.nl
T +31 (0)6 30 08 30 94

Martijn Annink
Senior Manager Ondernemingsrecht
E martijn.annink@bdo.nl
T +31 (0)6 24 65 83 91

09/2025 – FL25126