ONLINE TRUST COALITIE

Wetgevingsoverzicht Online Trust Coalitie

VERSIE 0.5 | LAATST BIJGEWERKT OP 26 APRIL 2024

Missie

De missie van de Online Trust Coalitie is het realiseren én behouden van vertrouwen in de clouddiensten. Door publiek-private samenwerking werken we aan een uniforme, gestandaardiseerde en geharmoniseerde aanpak, zodat aanbieders betrouwbaarheid kunnen aantonen en afnemers gemakkelijk kunnen vaststellen dat er van betrouwbaarheid sprake is.

Strategie

We geven uitvoering aan onze missie door Nederlandse oplossingen te verankeren in het Europees beleid rond cloud en cybersecurity. Nederland maakt daarbij met haar traditie in auditing, assurance en accounting, gebruik van haar voortrekkersrol. De OTC kiest voor een brede multi-stakeholder aanpak waarbij coalitiepartners gestimuleerd worden zelf aan de gang te gaan met de actiepunten en resultaten. De OTC stelt zich niet op als een formeel adviescollege maar probeert doorbraken te creëren door de concrete toepassing van praktische oplossingen en de uitwisseling van feiten, cijfers en inhoudelijke argumenten met alle relevante belanghebbenden in Nederland en de EU. Het is mede aan de OTC om te zorgen dat Nederlandse initiatieven in de pas blijven lopen met de ontwikkelingen in de EU.

Visie

De visie van de OTC is gebaseerd op drie pijlers: **Criteria, Controle en Communicatie.** Een betrouwbare cloud vereist dat clouddiensten aantoonbaar voldoen aan eisen die wij stellen als gebruikers en als maatschappij. Deze **criteria** worden gesteld in de vorm van regulering (zoals EUCS) of zelfregulering. Door onafhankelijk bewijs, dat tot stand komt door de nodige interne en externe **controle**, kunnen we met voldoende zekerheid stellen dat aan de gestelde eisen voldaan wordt. Dat is de kern van de assurance-gedachte. Uiteindelijk moet begrijpbare **communicatie,** bijvoorbeeld in de vorm van auditrapporten of certificaten, zorgen dat leveranciers van clouddiensten, op een geharmoniseerde manier, kunnen aantonen dat hun diensten voldoende betrouwbaar zijn.

Wetgevingsoverzicht

Nieuwe wet- en regelgeving voor de digitale economie zoals de aankomende CRA, de AI-Act, data-act, NIS2, spreken allemaal over certificeringen, normen, standaarden en afsprakenstelsels. Soms verwijzen ze naar de CSA (Cyber Security Act), maar zelden naar de drie pijlers: het daadwerkelijk verkrijgen van zekerheid, naar herbruikbaarheid en harmonisatie. Het is belangrijk om te monitoren welke richting die wetgeving op gaat, en of de OTC met inbrengen van kennis en de 3 pijlers, kan bijdragen aan betere uitvoerbaarheid en effectiviteit van die reguleringen.
Dit overzicht geeft een globaal inzicht in de huidige en toekomstige wetgeving van de Europese Unie, die Europa voorbereidt op de digitale toekomst. Belangrijk om te benadrukken is dat deze onderwerpen niet langer uitsluitend aan de IT-afdeling worden overgelaten. Bestuurders spelen hierin een leidende rol en dienen verantwoordelijkheid te nemen.

Disclaimer

De lezer van dit overzicht van wetgeving kan in geen enkel geval rechten ontlenen aan de informatie hierin verstrekt. Het betreft geen volledig overzicht, maar dient als richtlijn voor clouddienstverleners, gebruikers van clouddiensten en toezichthouders die te maken hebben met

diverse Europese wetgeving. Het is belangrijk op te merken dat slechts een beperkte selectie van relevante wetgeving wordt weergegeven en dat er nog vele sectorspecifieke en/of diensten specifieke Europese wetten bestaan die niet zijn opgenomen. Bovendien richt dit overzicht zich op bepaalde aspecten van de wetgeving, zonder volledig uitputtend te zijn over de behandelde onderwerpen. Onderdelen van dit wetgevingsoverzicht kunnen aan verandering onderhevig zijn, daarom wordt dit overzicht van tijd tot tijd bijgehouden. Raadpleeg altijd de meest recente versie.

Colofon

www.onlinetrustcoalitie.nl

Europese wetgeving in de IT-sector

In de snel evoluerende wereld van informatietechnologie (IT) is Europese wetgeving van cruciaal belang om gelijke tred te houden met technologische vooruitgang en de bescherming van de rechten van individuen te waarborgen. Momenteel bestaat er een veelvoud aan Europese wetgeving op dit gebied, terwijl er ook nog toekomstige wetgeving wordt ontwikkeld om te voldoen aan de voortdurend veranderende behoeften van de samenleving.

Het totstandkomingsproces van Europese wetgeving

Het proces van wetgevingsvorming op Europees niveau is complex en omvat op hoofdlijnen de volgende stappen:

1. **Voorstelfase**: Het proces begint meestal met een voorstel van de Europese Commissie, de uitvoerende tak van de Europese Unie. Dit voorstel kan voortkomen uit verschillende bronnen, zoals verzoeken van lidstaten, belangengroepen, of de eigen prioriteiten van de Commissie.

2. **Beoordeling en amendement**: Het voorstel wordt vervolgens beoordeeld en geamendeerd door zowel het Europees Parlement als de Raad van de Europese Unie. Tijdens deze fase vindt de triloog plaats, een informeel onderhandelingsproces tussen de Europese Commissie, het Europees Parlement en de Raad van de Europese Unie, waarbij compromissen worden gesloten over specifieke aspecten van het wetgevingsvoorstel. Dit proces stelt de instellingen in staat om consensus te bereiken voordat een definitieve versie van de wetgeving wordt aangenomen.

3. **Goedkeuring**: Zodra overeenstemming is bereikt tussen het Europees Parlement en de Raad van de Europese Unie, wordt de wet aangenomen. Afhankelijk van het type wetgeving kan deze worden aangenomen met gekwalificeerde meerderheid, unanimiteit, of in sommige gevallen, met instemming van alle lidstaten.

4. **Implementatie in lidstaten (met comitologie)**: Na goedkeuring moeten de lidstaten de wetgeving implementeren in hun nationale wetgevingssystemen. Tijdens dit proces kan de Europese Commissie gebruikmaken van comités van vertegenwoordigers van de lidstaten, zoals beheerscomités en regelgevingscomités, om bijstand te verlenen bij de uitvoering van specifieke taken en om ervoor te zorgen dat de wetgeving consistent wordt toegepast en uitgevoerd in alle lidstaten.

Doorwerking van verschillende Europese wetgeving

De doorwerking van Europese wetgeving in lidstaten verschilt afhankelijk van het type wetgeving. Hieronder volgt een uiteenzetting.

- Verordeningen: Verordeningen hebben directe werking in alle lidstaten zonder dat nationale implementatie nodig is. Dit betekent dat ze automatisch en onmiddellijk van kracht zijn in de nationale wetgeving van alle lidstaten, wat zorgt voor een uniforme toepassing binnen de hele EU.

- Richtlijnen: Richtlijnen daarentegen vereisen nationale implementatie. Elke lidstaat moet nationale wetgeving aannemen om aan de doelstellingen van de richtlijnen te voldoen, maar ze hebben de vrijheid om de specifieke middelen en methoden te kiezen om deze doelen te

bereiken. Hierdoor kan de implementatie enigszins variëren tussen lidstaten, wat kan leiden tot verschillen in nationale wetgeving en praktijken.

- Aanbevelingen: Aanbevelingen, hoewel niet-bindend, fungeren als instrumenten voor de EU om lidstaten richtlijnen te geven over specifieke kwesties. Ze hebben geen directe juridische gevolgen, maar kunnen worden gebruikt als leidraad voor nationale beleidsvorming en praktijken.

DSA Digital Services Act (regulation)	Bron http://data.europa.eu/eli/reg/2022/2065/oj

Doelgroep

Aanbieders van tussenhandeldiensten (online tussenpersonen), zijnde mere conduit-, caching-, en hostingdiensten. Denk aan internettoegangproviders, clouddienstverleners, online platforms waarop gebruikers informatie uitwisselen (social media), online handelsplatforms waarop vraag en aanbod bij elkaar wordt gebracht (Marktplaats, Bol.com) en online zoekmachines (Google, Bing).
Niet alle bepalingen uit de DSA zijn op alle bovengenoemde aanbieders van toepassing.

Van toepassing vanaf

De DSA is stapsgewijs ingevoerd. Sinds 25 augustus 2023 gelden voor de 19 allergrootste platforms en zoekmachines (met maandelijks gemiddeld meer dan 45 miljoen actieve gebruikers in de EU) strengere verplichtingen.
Sinds 17 februari 2024 is de DSA van toepassing op alle tussenhandelsdiensten, ongeacht hun grootte.

Impact

De DSA verheldert aansprakelijkheidsregels en introduceert due diligence verplichtingen voor online tussenpersonen. Het gaat om een asymmetrisch verplichtingenpakket: er zijn algemene regels en specifieke regels voor bijvoorbeeld online platforms die consumenten en handelaren samenbrengen. Hoe meer impact een partij kan hebben als tussenpersoon op consument en maatschappij, hoe groter en zwaarder de verplichtingen waaraan moet worden voldaan.
Volgens de DSA moeten bepaalde online tussenpersonen illegale inhoud en desinformatie gericht aanpakken, content aanbevelingssystemen mogelijk aanpassen, organisatorische zaken regelen (zoals het reageren en communiceren over illegale inhoud), rapportage- en informatieverplichtingen nakomen (zoals elk jaar de risico's van schadelijke onlinepraktijken op hun diensten beoordelen), informatie geven over specifieke onderwerpen en procedures in de algemene voorwaarden, contactpunten introduceren voor autoriteiten en consumenten.

Toezicht en handhaving NL en EU

De Europese Commissie zal, in samenwerking met de nationale autoriteiten, de handhaving van wetgeving coördineren, met speciale aandacht voor de naleving door online platforms binnen hun respectieve rechtsgebieden. Primair zal de Commissie verantwoordelijk zijn voor het toezicht op en de handhaving van bijkomende verplichtingen voor zeer grote online platforms en zoekmachines. Deze verplichtingen omvatten onder andere maatregelen ter beperking van systeemrisico's. In Nederland gaan de Autoriteit Consument & Markt (ACM) en de Autoriteit Persoonsgegevens (AP) toezicht houden op de DSA.
De lidstaten moeten ervoor zorgen dat de sancties voor het niet naleven van de verordening niet hoger zijn dan 6% van de jaarlijkse inkomsten of omzet van tussenhandelsdienstaanbieders, terwijl sancties voor het verstrekken van onjuiste informatie, niet reageren op correcties of inspecties ter plaatse niet hoger mogen zijn dan 1% van de jaarlijkse inkomsten of omzet van de betrokken dienstverlener.

Raakvlakken andere wetgeving

De DSA regelt hoe online tussenpersonen moeten omgaan met meldingen over vermeend illegale informatie binnen hun diensten. Voor online handelsplatforms, waar vraag en aanbod bij elkaar komt, gelden inrichtingseisen. De DSA heeft hierom raakvlakken met de verplichting van hostingdiensten om content te verwijderen met betrekking tot seksueel misbruik van kinderen en/of van terroristische aard zijn ((EU) 2021/784 en (EU) 2022/209) en de inrichtingseisen die specifiek voor onlinemarktplaatsen gelden (RICHTLIJN 2011/83/EU).

DMA Digital Markets Act (Regulation)	Bron http://data.europa.eu/eli/reg/2022/1925/oj

Doelgroep

Poortwachters die kernplatformdiensten aanbieden. Een platform valt als poortwachter onder de DMA als het dezelfde kernplatformdienst in ten minste 3 EU-lidstaten levert en in de laatste 3 jaar een jaaromzet van € 7,5 miljard in de EU heeft gerealiseerd of als het een marktwaarde heeft van minstens € 75 miljard in het afgelopen jaar. Ook moet zo'n platform gedurende 3 jaar ten minste 45 miljoen actieve eindgebruikers hebben en ten minste 10.000 zakelijke gebruikers die in de EU gevestigd zijn.
Per 6 september 2023 zijn 6 poortwachters en 22 van hun diensten aangewezen: Alphabet (met diensten zoals Google Search en YouTube), Amazon, Apple (met onder andere de App Store), ByteDance (TikTok), Meta (waaronder Facebook en WhatsApp), en Microsoft (met onder andere Windows en LinkedIn).

Van toepassing vanaf

Op 1 november 2022 is de DMA in werking getreden. Met ingang van 2 mei 2023 is de DMA ook daadwerkelijk van toepassing.

Impact

De DMA bevat aanvullende concurrentieregels voor een beperkt aantal online platforms die een zeer groot marktaandeel hebben. Deze platforms hebben een dusdanige positie dat zij als het ware fungeren als 'poortwachter' voor het internet: als ondernemer kan je bijna niet om deze platforms heen. Voor de poortwachters gelden o.a. aanvullende regels om eerlijke toegang en gebruik van hun diensten te waarborgen. Enkele voorbeelden van wat poortwachters moeten doen: eerlijke voorwaarden bieden aan ondernemers wanneer zij apps in de appstore van het platform aanbieden, ondernemers op aanvraag gratis toegang geven tot hun eigen data (ook klantgegevens), ondernemers toegang geven tot gegevens over hoe goed hun advertenties het doen op het platform, zorgen dat bijvoorbeeld apps en betaaldiensten van ondernemers kunnen aansluiten op (interoperabel zijn met) het besturingssysteem en de hardware van de poortwachter.
Enkele voorbeelden van wat poortwachters niet mogen doen: ondernemers verbieden om producten of diensten op hun eigen website of een ander platform voor een lagere prijs aan te bieden of met betere voorwaarden (dit heet ook wel een pariteitsclausule), eigen producten en diensten voortrekken of beter behandelen dan vergelijkbare producten of diensten van ondernemers in de zoekresultaten, ondernemers verplichten om bepaalde aanvullende diensten te gebruiken (zoals het gebruik van de betaaldienst van de poortwachter bij aankopen in apps), gegevens die het platform van ondernemers verzamelt met de ene dienst, gebruiken in concurrentie met die ondernemer bij een andere dienst (bijvoorbeeld bij digitale advertenties), ondernemers tegenhouden om buiten de appstore om te communiceren met klanten en abonnementen aan te bieden.

Toezicht en handhaving NL en EU

De Commissie heeft de belangrijkste rol bij het handhaven van de DMA. Naast het uitvoeren van marktonderzoek, krijgt de Europese Commissie ook verschillende onderzoeksbevoegdheden, zoals het vragen om informatie en het uitvoeren van inspecties. Daarnaast kan de Commissie voorlopige maatregelen nemen en, na het presenteren van voorlopige bevindingen, zowel gedragsmaatregelen als aanzienlijke geldboetes en dwangsommen opleggen bij overtreding van de DMA. Deze boetes kunnen oplopen tot 10% van de wereldwijde omzet, en zelfs meer dan 20% voor herhaalde overtreders. Bij herhaalde overtredingen binnen acht jaar kan de Commissie na marktonderzoek ook structurele maatregelen opleggen, zoals tijdelijke verboden op nieuwe fusies.
Nationale autoriteiten hebben een ondersteunende rol bij het toezicht op de naleving van de DMA. In Nederland is de Autoriteit Consument en Markt ("ACM") aangewezen als de nationale autoriteit. De ACM heeft verschillende toezichtsbevoegdheden en kan zelfstandig onderzoek doen, maar rapporteert uiteindelijk aan de Commissie. Alleen de Commissie kan vervolgens een handhavingsprocedure starten.

Raakvlakken andere wetgeving

Niet van toepassing.

NIS2 Network and Information Security Directive II (Directive)	Bron http://data.europa.eu/eli/dir/2022/2555/oj

Doelgroep

Belangrijke en essentiele entiteiten die actief zijn in zeer kritieke sectoren of andere kritieke sectoren. Volgens NIS2 vallen de volgende sectoren onder "zeer kritieke sectoren": energie; vervoer; bankwezen; infrastructuur voor de financiële markt; gezondheidszorg; drinkwater; afvalwater; digitale infrastructuur; beheer van ICT-diensten (business-to-business); overheid en ruimtevaart.
"Andere kritieke sectoren" zijn: post- en koeriersdiensten; afvalstoffenbeheer; vervaardiging, productie en distributie van chemische stoffen; productie, verwerking en distributie van levensmiddelen; vervaardiging; digitale aanbieders en onderzoek.

Een entiteit wordt als belangrijk beschouwd wanneer deze:

- Actief is in een zeer kritieke sector en een “middelgrote” organisatie is van 50 – 249 personen met een jaaromzet van €10 miljoen tot €50 miljoen of een balanstotaal van €10 - €43 miljoen.

Óf

- Actief is in een sector genoemd in een andere kritieke sector; en “grote” of “middelgrote” organisatie is op basis van bovengenoemde criteria.

Een entiteit wordt als essentieel beschouwd wanneer deze:

- Actief is in een zeer kritieke sector; en een “grote” organisatie is van 250 personen of meer, of een jaaromzet heeft van meer dan €50 miljoen en een balanstotaal boven de €43 miljoen.

Verder kunnen partijen ook essentieel zijn als ze op andere gronden worden aangewezen.

Van toepassing vanaf

NIS2 is van toepassing vanaf 16 januari 2023. Europese lidstaten hebben tot 17 oktober 2024 om hun nationale wet- en regelgeving in overeenstemming te brengen met de richtlijn. In Nederland zal hiervoor de Wet beveiliging van netwerk- en informatiesystemen (Wbni) worden aangepast. De overheid heeft aangekondigd dat ze de officiële deadline niet gaan halen. Daarom wordt verwacht dat organisaties begin 2025 moeten voldoen aan de geïmplementeerde wet.

Impact

NIS2 legt onder andere de volgende verplichtingen op:

- Registratieplicht: entiteiten moeten bij de bevoegde autoriteit o.a. KVK-gegevens, en IP-adressen registreren.
- Meldplicht: Bedrijven en overheidsorganisaties die onder NIS2 vallen, moeten incidenten die aanzienlijke verstoring van essentiële diensten kunnen veroorzaken, binnen 24 uur melden bij de toezichthouder. Daarnaast dienen cyberincidenten te worden gemeld bij het Computer Security Incident Response Team (CSIRT), dat vervolgens ondersteuning kan bieden. Factoren die een incident meldingswaardig maken, omvatten onder andere het aantal getroffen personen, de duur van de verstoring en mogelijke financiële verliezen.
- Zorgplicht: De richtlijn verplicht entiteiten om zelf een risicobeoordeling uit te voeren. Op basis daarvan dienen ze passende maatregelen te nemen om de continuïteit van hun diensten te waarborgen en de veiligheid van de gebruikte informatie te waarborgen. Maatregelen voor het beheer van cyber- en beveiligingsrisico’s zijn bijvoorbeeld: risicoanalyses, incidentenbehandeling, bedrijfscontinuïteit, beveiliging van de toeleveringsketen, beveiliging bij het verwerken van gegevens, het ontwikkelen en onderhouden van netwerk- en

informatiesystemen, het opstellen van beleid en procedures om de effectiviteit van maatregelen voor het beheer van cyberbeveiligingsrisico's te beoordelen, basispraktijken op het gebied van cyberhygiëne en opleiding op het gebied van cyberbeveiliging, beleid inzake het gebruik van cryptografie en encryptie, beveiligingsaspecten voor personeel, toegangsbeleid en beheer van activa, wanneer gepast, gebruik van MFA of continue- authenticatieoplossingen, beveiligde spraak-, video- en tekstcommunicatie en beveiligde nood- en communicatiesystemen binnen de organisatie.

- Governance: bestuurders moeten meer betrokken zijn bij cyberveiligheid van hun organisatie. Bestuurders moeten aandacht besteden aan hun kennisniveau van cyberveiligheid door een opleiding te volgen.

Het voldoen aan bestaande kaders voor informatiebeveiliging bij de overheid, waaronder de Baseline Informatiebeveiliging Overheid (BIO), dient als basis om invulling te geven aan de zorgplicht die voortvloeit uit NIS2. Het naleven van de huidige verplichtingen vormt dus een cruciaal startpunt.

Voor overheidsinstanties betekent dit dat de invulling van de NIS2-zorgplicht zoveel mogelijk zal plaatsvinden binnen de grenzen van bestaande kaders. Organisaties die voorheen niet aan de bestaande kaders voor informatiebeveiliging voldeden, hebben nu vanuit NIS2 wel de verplichting om dit te doen.

Belangrijk is de nuance dat dat niet alle bepalingen uit de NIS2-richtlijn voor iedere partij van toepassing is. Zo is de registratieplicht zeer beperkt van toepassing (afhankelijk van de aard van de diensten die een partij levert), een zorgpartij hoeft zich bijvoorbeeld niet te registreren, maar een DNS-dienstverlener wel.

Toezicht en handhaving NL en EU

Lidstaten moeten zelf een toezichthouder aanwijzen. Momenteel is niet bekend welke partij toezichthouder wordt in Nederland. Lidstaten moeten ervoor zorgen dat de toezichthouder onder andere de mogelijkheid krijgt om bindende instructies en bevelen te geven, en om administratieve boetes op te leggen. De maximale hoogte van deze boetes moet door de lidstaten worden vastgesteld op maximaal €10 miljoen of 2% voor essentiële entiteiten en maximaal €7 miljoen of 1.4% voor belangrijke entiteiten van de totale wereldwijde omzet, afhankelijk van welk bedrag hoger is. Bovendien kunnen bestuurders aansprakelijk worden gesteld als zij de NIS2-richtlijn niet naleven.

Raakvlakken andere wetgeving

NIS2 heeft bijvoorbeeld raakvlakken met DORA. DORA fungeert als een aanvullende maatregel op bestaande wetgeving, waaronder NIS2, met betrekking tot financiele instellingen en bedrijven aanverwante ICT-diensten leveren.
In het kader van NIS2 kan cybersecurity certificering onder de CSA verplicht gesteld worden.
Verder heeft NIS2 raakvlakken met Eidas, want de Eidas bepaalt dat de aanbieders van vertrouwensdiensten opgelegde cyberbeveiligingsvoorschriften moet stroomlijnen met het in de NIS2-richtlijn opgericht wettelijke kader. Daarvoor moeten vertrouwensdiensten passende technische en organisatorische maatregelen nemen overeenkomstig NIS2-richtlijn, zoals maatregelen tegen systeemfalen, menselijke fouten, kwaadwillige acties of natuurverschijnselen, om de risico's te beheren voor de beveiliging van netwerk- en informatiesystemen die die aanbieders gebruiken om hun diensten te verlenen, en om significante incidenten en cyberbedreigingen te melden overeenkomstig de NIS2-richtlijn.
Ook heeft NIS2 raakvlakken met de CER-richtlijn, die zich richt zich op de bescherming van organisaties tegen fysieke dreigingen, zoals de gevolgen van (terroristische) misdrijven, sabotage en natuurrampen. De NIS2-richtlijn richt zich op digitale (cyber) risico's voor netwerk- en informatiesystemen, zoals het internet en het betalingsverkeer. Tezamen dienen ze de fysieke, digitale en economische weerbaarheid van Europese lidstaten ten aanzien van deze dreigingen te versterken.

AI Act Artificial Intelligence Act (Regulation)	Bron https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52021PC0206

Doelgroep

Aanbieders die AI-systemen in de EU in de handel brengen of in gebruik stellen en aanbieders van AI-systemen die zich buiten de EU bevinden wanneer de output van het AI-systeem in de EU wordt gebruikt. Daarnaast ook distributeurs, importeurs, gebruikers en eventueel derden die met AI-systemen te maken hebben.

Van toepassing vanaf

De AI Act is in maart 2024 definitief aangenomen. Op het moment van schrijven moet de wettekst nog worden gefinaliseerd. Als de tekst is gefinaliseerd dan wordt deze gepubliceerd in de Official Joural (het Staatsblad van de EU), 21 dagen daarna wordt de AI Act definitief wet. De AI Act zal 2 jaar daarna (dus ergens in 2026) in alle lidstaten van toepassing worden.
Let op: de verboden praktijken (AI met onacceptabele risico's) moeten binnen 6 maanden stoppen nadat de AI Act definitief wet is geworden.

Impact

Alle inzet van AI valt onder de AI Act. De verordening volgt een risico gebaseerde benadering en legt verplichtingen op aan aanbieders en gebruikers afhankelijk van het risiconiveau dat een AI-systeem met zich meebrengt. De AI Act is van toepassing op alle sectoren en is niet beperkt tot een specifieke branche. Op hoofdlijnen wordt onderscheid gemaakt tussen AI-systemen met:
Onacceptabele risico's: als een AI iets doet dat in strijd is met Europese fundamentele normen en waarden, dan mag deze niet op de Europese markt ingezet worden. Een voorbeeld is predictive policing; AI laten voorspellen of iemand crimineel gedrag zal gaan vertonen. Er is wel enige ruimte voor biometrische surveillance, onder strikte voorwaarden.
Hoge risico's: AI-systemen die een hoog risico vormen voor de gezondheid, veiligheid, grondrechten of het milieu zijn toegestaan mits wordt voldaan aan strenge voorwaarden. Zo moet duidelijk zijn waar de data vandaan komt waarmee de AI is getraind, is menselijk toezicht vereist en moet de technische documentatie op orde zijn. Het afhandelen van verzekeringsclaims, bepaalde medische hulpmiddelen en algoritmes die sollicitanten beoordelen zijn voorbeelden van hoog risico-AI.
Lage risico's: AI-systemen die niet onder de voorafgaande categorieën vallen, mogen zonder al te veel problemen de Europese markt op. De AI moet wel transparant zijn, zodat niemand denkt met een mens te maken te hebben, en de AI mag geen beslissingen nemen.
Specifiek transparantierisico: algemene AI modellen en foundation modellen zoals GPT en Bard.
AI-systemen met onacceptabele risico's zijn verboden.
Veruit de meeste verplichtingen gelden voor AI-systemen die in de categorie hoog vallen. Het volgende moet onder andere geregeld zijn:

- Fundamental Rights Impact Assessment: vooraf moeten gestructureerd de risico’s in kaart worden gebracht voor kwesties als veiligheid, privacy, discriminatie, eerlijke toegang tot zorg, onderwijs en belangrijke diensten.
- Risicomanagementsysteem: om potentiële risico's te identificeren, evalueren, beheren en verminderen.
- Systeem voor gegevensbeheer: er moet gebruik worden gemaakt van onbevooroordeelde, kwalitatieve en representatieve datasets.
- Technische documentatie: voor gebruikers moet duidelijk zijn hoe het AI-systeem gebruikt moet worden.

- Transparantie: voor gebruikers moet duidelijk zijn hoe het AI-systeem werkt. Zo geldt er ook een verplichting om te loggen om te kunnen traceren en controleren wat er precies is gebeurd.
- Menselijk toezicht: bij het gebruik van het AI-systeem is menselijk toezicht vereist.
- Conformiteitsbeoordeling: er geldt een specifieke conformiteitsbeoordelingsprocedure die verschilt van het huidige CE-markeringssysteem voor andere producten. Het doel is om een beoordelingsproces te hebben dat is afgestemd op de unieke kenmerken en risico's van AI-systemen.

Voor AI-systemen met een laag risico gaan er onder meer transparantieverplichtingen gelden. Bovenstaande verplichtingen rusten niet op één partij; de AI Act kent verschillende rollen en elke rol kent eigen verantwoordelijkheden.

Toezicht en handhaving NL en EU

De AI Act vereist dat er een nationale toezichthoudende autoriteit wordt aangewezen door ieder lidstaat, die samenwerkt met nationale bevoegde instanties om ervoor te zorgen dat de AI Act wordt nageleefd. Deze nationale toezichthoudende autoriteit maakt deel uit van de European AI Board (EAIB). Momenteel is nog niet bekend welke partij de Nederlandse toezichthouder wordt voor de naleving van de AIA. Dit wordt waarschijnlijk binnen 3 maanden na inwerkingtreding bekendgemaakt.

Een nationale toezichthouder kan 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.
Bovendien moeten lidstaten ook boetes vaststellen binnen de grenzen die zijn vastgesteld in de AI Act. Dat is €35 miljoen of bij bedrijven 7% van wereldwijde concernomzet bij inzet van verboden AI, €15 miljoen of bij bedrijven 3% van wereldwijde concernomzet bij andere overtredingen €7,5 miljoen of bij bedrijven 1,5% van wereldwijde concernomzet bij verstrekken van onjuiste informatie over risicostatus of bij transparantievereisten.

Voor mkb en startups zullen lagere plafonds gaan gelden.

Raakvlakken andere wetgeving

Waar de AR beoogt consumenten te beschermen tegen schade door een gebrekkig product (waaronder digitale diensten) vult de AILD de AR aan door specifiek de bewijslast voor consumenten te verlichten die schade hebben ondervonden door een AI-systeem. De AILD vult op haar beurt daarmee de AI Act aan. Door consumenten een mogelijkheid te bieden om schade te verhalen door bijvoorbeeld een AI-systeem die onacceptabele risico's heeft veroorzaakt en niet uit de Europese markt is gehaald.

AR Aansprakelijkheidsrichtlijn (Directive)	Bron https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX%3A52022PC0495

Doelgroep

Fabrikanten (en diens importeurs en/of vertegenwoordigers) van producten, waaronder ook ontwikkelaars (en diens importeurs en/of vertegenwoordigers) van digitale fabricage en software worden begrepen (met uitzondering van ontwikkelaars open source software).

Van toepassing vanaf

De nieuwe productaansprakelijkheidsrichtlijn is op het moment van schrijven nog niet definitief aangenomen. Onduidelijk is wanneer deze in werking treedt.

Impact

In de nieuwe productaansprakelijkheidsrichtlijn zijn verschillende belangrijke wijzigingen opgenomen om een betere bescherming van consumenten te waarborgen en om gelijke regelgeving binnen de EU te bevorderen.
De definitie van een product wordt uitgebreid om ook software, kunstmatige intelligentie en digitale diensten zoals robots, drones en slimme-huis systemen te omvatten. Open source of vrije software valt echter buiten deze regels vanwege hun afhankelijkheid van gebruikersverbeteringen, waardoor ontwikkelaars niet aansprakelijk kunnen worden gesteld.
Een van de belangrijkste veranderingen is dat de bewijslast voor slachtoffers in complexe zaken wordt verlicht, waardoor het gemakkelijker wordt om schadevergoeding te verkrijgen. Daarnaast kunnen fabrikanten nu verplicht worden om bewijsmateriaal openbaar te maken in geval van gebrekkige producten.
De herziene richtlijn voorziet ook in compensatie voor medisch erkende psychologische schade en voor de vernietiging of onomkeerbare beschadiging van gegevens. Verder stelt de richtlijn vast dat er altijd een aansprakelijkheid moet zijn binnen de EU voor schade veroorzaakt door een defect product, zelfs als het buiten de EU is vervaardigd. Dit kan de gemachtigde vertegenwoordiger van de fabrikant of, in laatste instantie, de fulfilment-dienstverlener (een onderneming die doorgaans opslag-, verpakkings- en verzendingsdiensten verleent) aansprakelijk worden gesteld. Als er geen aansprakelijk bedrijf is, kunnen consumenten nog steeds compensatie krijgen via nationale regelingen.
Al met al beoogt de richtlijn een consistente regelgeving vast te stellen voor alle lidstaten, met als doel een goed functionerende digitale en circulaire economie te bevorderen en slachtoffers van beschadigde of defecte producten te helpen bij het verkrijgen van een rechtvaardige schadevergoeding.

Toezicht en handhaving NL en EU

Voor deze regelgeving wordt geen toezichthouder aangesteld. Deze wetgeving kan in een burgerlijke rechtzaak worden gebruikt om causaliteit te veronderstellen, waardoor de bewijslast voor slachtoffers kan worden verlicht.

Raakvlakken andere wetgeving

Waar de AR beoogt consumenten te beschermen tegen schade door een gebrekkig product (waaronder digitale diensten) vult de AILD de AR aan door specifiek de bewijslast voor consumenten te verlichten die schade hebben ondervonden door een AI-systeem. De AILD vult op haar beurt daarmee de AI Act aan. Door consumenten een mogelijkheid te bieden om schade te verhalen door bijvoorbeeld een AI-systeem die onacceptabele risico's heeft veroorzaakt en niet uit de Europese markt is gehaald.

AILD Artificieel Intelligence Liability Directive (Directive)	Bron https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0496

Doelgroep

Aanbieders die AI-systemen in de EU in de handel brengen of in gebruik stellen en aanbieders van AI-systemen die zich buiten de EU bevinden wanneer de output van het AI-systeem in de EU wordt gebruikt. Daarnaast ook distributeurs, importeurs, gebruikers en eventueel derden die met AI-systemen te maken hebben.

Van toepassing vanaf

De AILD is op het moment van schrijven nog niet definitief aangenomen. Als de AILD eenmaal is aangenomen zullen de lidstaten naar verwachting 2 jaar de tijd krijgen om de hun nationale wet- en regelgeving in overeenstemming te brengen met de richtlijn.

Impact

De AILD bevat een algemeen kader voor niet-contractuele aansprakelijkheid bij schade veroorzaakt door AI-systemen. De AILD beoogt ervoor te zorgen dat personen die schade ondervinden door AI-systemen dezelfde mate van bescherming genieten als personen die schade ondervinden door andere technologieën in de EU. De AI-aansprakelijkheidsrichtlijn zou een (weerlegbare) veronderstelling van causaliteit creëren om de bewijslast voor slachtoffers te verlichten bij het aantonen van schade veroorzaakt door een AI-systeem. Bovendien zou het nationale rechtbanken de bevoegdheid geven om openbaarmaking van bewijsmateriaal over vermoedelijk schadelijke AI-systemen te bevelen.

Toezicht en handhaving NL en EU

Voor deze regelgeving wordt geen toezichthouder aangesteld. Deze wetgeving kan in een burgerlijke rechtszaak worden gebruikt om causaliteit te veronderstellen, waardoor de bewijslast voor slachtoffers kan worden verlicht.

Raakvlakken andere wetgeving

Waar de AR beoogt consumenten te beschermen tegen schade door een gebrekkig product (waaronder digitale diensten) vult de AILD de AR aan door specifiek de bewijslast voor consumenten te verlichten die schade hebben ondervonden door een AI-systeem. De AILD vult op haar beurt daarmee de AI Act aan. Door consumenten een mogelijkheid te bieden om schade te verhalen door bijvoorbeeld een AI-systeem die onacceptabele risico's heeft veroorzaakt en niet uit de Europese markt is gehaald.

CRA Cyber Resilience Act (Regulation)	Bron https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0454

Doelgroep

Fabrikanten, importeurs en distributeurs van producten met digitale elementen die in verbinding staan met andere apparaten of een netwerk.

Van toepassing vanaf

Op 12 maart 2024 heeft het Europees Parlement de CRA goedgekeurd. De CRA moet nu formeel worden aangenomen door de Europese Raad om van kracht te worden. Dit wordt verwacht in april 2024.

Na inwerkingtreding hebben fabrikanten, importeurs en distributeurs van producten met digitale elementen 36 maanden de tijd om zich aan de nieuwe vereisten aan te passen. De verplichting voor fabrikanten om incidenten en kwetsbaarheden te melden wordt echter 21 maanden na inwerkingtreding van kracht

Impact

De CRA zorgt ervoor dat digitale producten, waaronder alle hardware (waar bepaalde software onderdeel van is), software en componenten, aan essentiële cybersecurityeisen voldoen voordat ze op de Europese markt worden gebracht.
De CRA stelt hieraan strenge eisen voordat ze op de markt worden gebracht. Deze eisen omvatten onder andere:

- Producten moeten veilig zijn ontworpen, ontwikkeld en geproduceerd (secure-by-design).
- Ze mogen geen bekende uitbuitbare kwetsbaarheden hebben.
- Standaardconfiguraties moeten veilig zijn (secure-by-default).
- Automatische updates moeten standaard zijn ingeschakeld.
- Producten moeten sterke authenticatie en autorisatie bieden, en gegevens moeten goed worden beschermd, bijvoorbeeld door encryptie.
- Gevoelige data moet worden geminimaliseerd en beschikbaarheid moet worden gewaarborgd, ook tegen DDOS-aanvallen.

Essentiële beveiligingseisen met betrekking tot het omgaan met kwetsbaarheden:

- Fabrikanten moeten kwetsbaarheden identificeren en documenteren.
- Kwetsbaarheden moeten direct worden aangepakt met gratis security-updates gedurende de levensduur van het product.
- Beveiliging moet regelmatig worden getest en beoordeeld.
- Kwetsbaarheden moeten publiekelijk worden bekendgemaakt na beschikbaarheid van een security-update.
- Fabrikanten moeten beleid vaststellen voor coordinated vulnerability disclosure en een veilig update-mechanisme bieden.

Meldplicht:

- Kwetsbaarheden en beveiligingsincidenten moeten actief worden gemeld.
- In geval van een incident moet binnen 24 uur een early warning worden gegeven, en binnen 72 uur een volledige melding van het incident.

Levensduur van producten:

- Leveranciers moeten de ondersteuningstermijn van producten vaststellen en proactief communiceren bij de verkoop, zowel voor digitale als fysieke producten.
- Toezichthouders zullen de gemiddelde verwachte levensduur van producten bijhouden en op geaggregeerd niveau communiceren.

Digitale producten die aan deze eisen voldoen mogen de CE-markering gebruiken om deze aan te bieden in de interne markt. In de meeste gevallen kunnen partijen zelf beoordelen of ze aan de vereisten voldoen. Echter, bij een selecte groep van cruciale producten is een beoordeling door een externe partij vereist. De specifieke lijst van deze kritieke producten is nog onderwerp van de laatste onderhandelingen en kan daarom nog niet worden verstrekt (raadpleeg bijlage 3 klasse 2).

Toezicht en handhaving NL en EU

De CRA voorziet toezichthouders van bevoegdheden om boetes op te leggen. Op dit moment is nog niet bekend welke partij in Nederland toezichthouder wordt.
Niet-naleving van cruciale verplichtingen met betrekking tot cybersecurity kan resulteren in boetes tot € 15 miljoen of 2,5% van de jaaromzet, afhankelijk van welk bedrag hoger is.
Voor andere overtredingen binnen de CRA zijn administratieve boetes mogelijk tot € 10 miljoen of 2% van de wereldwijde jaaromzet, indien dat bedrag hoger ligt. Het verstrekken van onjuiste informatie aan markttoezichthouders kan leiden tot een boete van € 5 miljoen of 1% van de wereldwijde jaaromzet in het voorgaande belastingjaar, wanneer dat bedrag hoger is.
Lidstaten hebben de vrijheid om aanvullende sancties op te leggen voor niet-naleving van de CRA, mits deze evenredig en effectief zijn, maar ze moeten deze regels aan de Europese Commissie melden.
Markttoezichthouders kunnen producten verbieden of beperken als fabrikanten, importeurs, distributeurs of andere verantwoordelijke bedrijven niet aan de vereisten voldoen. Ook de Europese Commissie heeft de bevoegdheid om maatregelen te treffen voor producten met digitale componenten die een aanzienlijk beveiligingsrisico vormen, waaronder het terugroepen of uit de handel nemen van deze producten binnen een redelijke termijn.

Raakvlakken andere wetgeving

Niet van toepassing.

CER Critical Entities Resilience Directive (Directive)	Bron http://data.europa.eu/eli/dir/2022/2557/oj

Doelgroep

De voorschriften zijn van toepassing uitsluitend op instellingen die door de overheid zijn aangeduid als vitale entiteiten. Een entiteit wordt beschouwd als vitaal wanneer zij essentiële diensten verleent binnen de sectoren van digitale infrastructuur (waaronder telecomaanbieders, topleveldomeinnaamregisters en cloudproviders), bankwezen, energie, transport, financiële marktinfrastructuur, gezondheidszorg, drinkwater- of afvalwaterbeheer, overheidsinstanties, ruimtevaart of de productie, verwerking en distributie van voedsel. Voorheen aangewezen als 'vitale aanbieders' binnen deze sectoren zullen ook worden herkend als vitale entiteiten.

Van toepassing vanaf

De termijn voor de integratie van de CER-richtlijn in het Nederlandse rechtssysteem verstrijkt op 17 oktober 2024. Organisaties zijn verplicht om binnen 10 maanden na hun aanwijzing als kritieke entiteit aan de voorschriften te voldoen.

Impact

De CER-richtlijn is opgesteld om kritieke organisaties beter bestand te maken tegen fysieke bedreigingen zoals terroristische aanslagen, rampen en klimaatverandering. Deze richtlijn legt diverse maatregelen voor veerkracht vast en vereist dat ernstige incidenten binnen 24 uur worden gemeld. Organisaties kunnen gebruikmaken van door de overheid verstrekte risicobeoordelingen om de juiste veerkrachtmaatregelen vast te stellen. Niet-naleving van de geïmplementeerde CER-richtlijn wordt bestraft.

Toezicht en handhaving NL en EU

De CER-richtlijn legt een aantal essentiële verplichtingen op, waaronder:

- Zorgplicht - Bedrijven dienen zelf een risicobeoordeling uit te voeren en op basis daarvan maatregelen te treffen om de continuïteit van hun dienstverlening te waarborgen en hun informatie te beschermen tegen fysieke dreigingen.
- Meldplicht - Bedrijven moeten incidenten die de essentiële dienstverlening aanzienlijk kunnen verstoren binnen 24 uur melden bij de toezichthouder. In geval van een cyberincident dient dit ook gemeld te worden bij het Computer Security Incident Response Team (CSIRT), dat vervolgens hulp en bijstand kan bieden. Of een incident onder de meldplicht valt, hangt af van verschillende factoren zoals het aantal getroffen personen, de duur van de verstoring en potentiële financiële verliezen.
- Toezicht - Organisaties die onder de CER-richtlijn vallen, worden onder toezicht geplaatst om te controleren of zij aan de verplichtingen van de richtlijn, zoals de zorg- en meldplicht, voldoen. Op dit moment wordt bepaald welke sectoren onder het toezicht van welke toezichthouder vallen.

Raakvlakken andere wetgeving

Deze richtlijn vult de NIS2-richtlijn aan, die gericht is op het versterken van digitale veerkracht.

DGA Data Governance Act (Regulation)	Bron http://data.europa.eu/eli/reg/2022/868/oj

Doelgroep

Openbare lichamen, aanbieders van databemiddelingsdiensten, organisaties voor data-altruïsme.

Van toepassing vanaf

De DGA is van toepassing sinds 24 september 2023. Aanbieders van databemiddelingsdiensten hebben nog tot 24 september 2025 om aan hun verplichtingen uit de DGA te voldoen.

Impact

De DGA introduceert nieuwe regels voor databemiddelingsdiensten die zich richten op het delen van data tussen gegevenshouders en gegevensgebruikers. Aanbieders van deze diensten moeten onder meer aan beveiligings- en interoperabiliteitseisen gaan voldoen. Daarnaast bevat de DGA een kader voor data-altruïsme: het verwerken van gegevens voor algemeen belang. Organisaties die zich hiermee bezighouden moeten onder meer aan eisen voldoen om de privacy en overige belangen van personen en bedrijven die gegevens beschikbaar stellen te beschermen. De DGA bevat ook aanvullende regels om de beschikbaarheid van overheidsinformatie te verbeteren.

Toezicht en handhaving NL en EU

De Autoriteit Consument en Markt (ACM) wordt de toezichthouder op naleving van de DGA. Bij hen zullen databemiddelingsdiensten zich ook moeten registreren. Bedrijven, organisaties en instellingen die zich bezighouden met het verwerken van data moeten zich aanmelden bij de beoogde toezichthouder ACM als ze hun diensten willen blijven aanbieden in de EU. Ze kunnen nu al een voorregistratie doen bij de ACM. Dat kan via deze website: https://www.acm.nl/nl/online-platforms/datadiensten.

Raakvlakken andere wetgeving

De DA en de Data Governance Act (DGA) versterken elkaar om betrouwbare en veilige toegang tot gegevens te vergemakkelijken en het gebruik ervan in belangrijke economische sectoren en gebieden van algemeen belang te bevorderen. De DGA regelt processen en structuren voor vrijwillige gegevensdeling, terwijl de DA bepaalt wie waarde kan creëren uit data en onder welke voorwaarden. Samen zullen deze twee wetgevingen helpen bij het creëren van een interne EU-markt voor gegevens.
De verhouding tussen de Algemene Verordening Gegevensbescherming (AVG), de Data Governance Act (DGA) en de Data Act (DA) draait om gegevensregulering. Omdat alle drie wetgevingen gegevens behandelen, kan er overlap zijn tussen hen. De AVG is specifiek van toepassing op persoonsgegevens, wat betekent dat gegevens die niet direct of indirect aan individuen kunnen worden gekoppeld, buiten het toepassingsgebied vallen. De DGA en de DA zijn breder en omvatten alle soorten gegevens. Ze hanteren ruimere definities van 'gegevens', waaronder persoonsgegevens. De DGA regelt bijvoorbeeld het hergebruik van niet-publiek toegankelijke overheidsgegevens, waarin zowel bedrijfsgeheimen, intellectuele eigendomsrechten als persoonsgegevens kunnen voorkomen. De DA is van toepassing op zowel persoonsgegevens als niet-persoonsgegevens.
Hoewel alle drie de verordeningen persoonsgegevens omvatten, rijst de vraag welke voorrang heeft bij een conflict tussen hen. Zowel de DGA als de DA stellen dat de AVG prevaleert bij inconsistenties.

DA Data Act (ook wel "Dataverordening" genoemd) (Regulation)	Bron https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2022:68:FIN

Doelgroep

Aanbieders van dataverwerkingsdiensten. Denk onder meer aan aanbieders van cloud- en edgediensten.

Van toepassing vanaf

Op 11 januari 2024 is de DA in werking getreden. Bedrijven hebben de tijd om zich voor te bereiden, aangezien de DA vanaf september 2025 van toepassing wordt.

Impact

De DA moet een uniform kader bieden voor het gebruiken en delen van data binnen de gehele EU. Dit wordt gerealiseerd door optimalisatie van toegankelijkheid en gebruik, en het stimuleren van een concurrerende en betrouwbare Europese cloudmarkt. Hieronder volgt aanvullende uitleg:
De DA legt specifieke regels op aan bedrijven die gegevens verzamelen of slimme apparaten verkopen. Hierbij ligt de nadruk op transparantie, toegang tot data, de mogelijkheid tot overstappen tussen clouddiensten, de bevoegdheid van de overheid om data op te eisen, en bepalingen in contracten.

Een cruciaal aspect van de DA is de verplichting voor producenten en verkopers om transparantie te bieden aan consumenten. Producten en diensten dienen zo ontworpen te zijn dat gegenereerde data standaard gemakkelijk en veilig toegankelijk is. Consumenten hebben het recht om deze data kosteloos te verkrijgen en kunnen ervoor kiezen deze met derden te delen, met beperkingen om misbruik te voorkomen.

Daarnaast richt de Data Act zich op het vergemakkelijken van de overstap tussen clouddiensten, waarbij grote providers zoals Google en Apple functionele gelijkwaardigheid moeten waarborgen. Hoewel een vergoeding in de eerste drie jaar is toegestaan, dient overstappen daarna kosteloos te zijn.

In bijzondere situaties kan de overheid data opeisen, met duidelijke criteria voor noodsituaties of taken van algemeen belang (zie hoofdstuk 5).

De DA heeft tevens invloed op contractuele bepalingen, waarbij verplichtingen worden opgelegd met betrekking tot overstappen naar andere diensten en het verbieden van clausules die strijdig zijn met goede handelspraktijken.

Wat betreft interoperabiliteitseisen vereist de DA dat exploitanten van dataruimtes compatibel zijn met andere dataruimtes, inclusief beschrijvingen van datastructuren, formaten en technische toegang.

Toezicht en handhaving NL en EU

Elk land binnen de EU moet één of meerdere autoriteiten aanwijzen die verantwoordelijk zijn voor het uitvoeren en handhaven van deze verordening. Ze kunnen ervoor kiezen om bestaande autoriteiten aan te wijzen of nieuwe autoriteiten op te richten. De Autoriteit Consument & Markt (ACM) en de Autoriteit Persoonsgegevens (AP) zijn aangewezen als nationale toezichthouder.

De toezichthoudende autoriteiten kunnen boetes opleggen voor overtredingen van deze verordening tot €20.000.000 tot 4% van de totale wereldwijde jaaromzet in het voorgaande boekjaar.

Specifiek voor overtredingen met betrekking tot het beschikbaar stellen van data aan overheidsinstanties en EU-instellingen, -agentschappen of -organen vanwege uitzonderlijke noodzaak, kan de toezichthoudende autoriteit boetes opleggen tot €50.000 per inbreuk en maximaal €500.000 per jaar. Verder kunnen de lidstaten nog aanvullende regels stellen op voor de straffen die gelden bij overtredingen van deze verordening en nemen alle vereiste maatregelen om ervoor te zorgen dat deze straffen worden gehandhaafd.

Raakvlakken andere wetgeving

De DA en de Data Governance Act (DGA) versterken elkaar om betrouwbare en veilige toegang tot gegevens te vergemakkelijken en het gebruik ervan in belangrijke economische sectoren en gebieden van algemeen belang te bevorderen. De DGA regelt processen en structuren voor vrijwillige gegevensdeling, terwijl de DA bepaalt wie waarde kan creëren uit data en onder welke voorwaarden. Samen zullen deze twee wetgevingen helpen bij het creëren van een interne EU-markt voor gegevens.

De verhouding tussen de Algemene Verordening Gegevensbescherming (AVG), de Data Governance Act (DGA) en de Data Act (DA) draait om gegevensregulering. Omdat alle drie wetgevingen gegevens behandelen, kan er overlap zijn tussen hen. De AVG is specifiek van toepassing op persoonsgegevens, wat betekent dat gegevens die niet direct of indirect aan individuen kunnen worden gekoppeld, buiten het toepassingsgebied vallen. De DGA en de DA zijn breder en omvatten alle soorten gegevens. Ze hanteren ruimere definities van 'gegevens', waaronder persoonsgegevens. De DGA regelt bijvoorbeeld het hergebruik van niet-publiek toegankelijke overheidsgegevens, waarin zowel bedrijfsgeheimen, intellectuele eigendomsrechten als persoonsgegevens kunnen voorkomen. De DA is van toepassing op zowel persoonsgegevens als niet-persoonsgegevens.

Hoewel alle drie de verordeningen persoonsgegevens omvatten, rijst de vraag welke voorrang heeft bij een conflict tussen hen. Zowel de DGA als de DA stellen dat de AVG prevaleert bij inconsistenties.

GDPR General Data Protection Regulation (Regulation)	Bron http://data.europa.eu/eli/reg/2016/679/oj

Doelgroep

Organisaties die zich binnen of buiten de EU bevinden, en persoonsgegevens verwerken van personen binnen de EU.

Van toepassing vanaf

De Nederlandse implementatie van de GDPR is de Algemene Verordening Gegevensverwerking (AVG). De AVG is inwerking getreden op 25 mei 2018

Impact

De GDPR/AVG is een Europese wet die de privacy van individuen beschermt door regels vast te stellen voor de verwerking van persoonsgegevens. De AVG formuleert de beginselen voor de verwerking van persoonsgegevens, namelijk:

- Rechtmatigheid, behoorlijkheid en transparantie: Persoonsgegevens moeten op een rechtmatige, behoorlijke en transparante wijze worden verwerkt. Dit houdt in dat de verwerking gebaseerd moet zijn op een geldige rechtsgrond, eerlijk moet zijn voor de betrokkenen en dat zij op de hoogte moeten zijn van hoe hun gegevens worden verwerkt.
- Doelbinding: Persoonsgegevens mogen alleen worden verzameld en verwerkt voor specifieke, duidelijke en rechtmatige doeleinden. Ze mogen niet verder worden verwerkt op een manier die onverenigbaar is met deze doeleinden.
- Gegevensminimalisatie: De verwerking van persoonsgegevens moet beperkt zijn tot wat noodzakelijk is voor de doeleinden waarvoor ze worden verwerkt. Organisaties moeten streven naar het verzamelen van alleen die gegevens die strikt nodig zijn.
- Nauwkeurigheid: Persoonsgegevens moeten accuraat en actueel zijn. Passende maatregelen moeten worden genomen om ervoor te zorgen dat onnauwkeurige gegevens zo snel mogelijk worden gecorrigeerd of verwijderd.
- Bewaarbeperking: Gegevens mogen niet langer worden bewaard dan noodzakelijk is voor de doeleinden waarvoor ze worden verwerkt. Organisaties moeten een beleid hebben voor de bewaartermijnen van persoonsgegevens.
- Integriteit en vertrouwelijkheid: Persoonsgegevens moeten op een manier worden verwerkt die adequate beveiliging waarborgt. Dit omvat bescherming tegen ongeoorloofde toegang, verlies, vernietiging of schade.

De AVG legt verplichtingen op aan organisaties die dergelijke gegevens verwerken en bepaalt de rechten van betrokkenen inzake hun persoonsgegevens. Als de ene partij persoonsgegevens namens de andere partij gaat verwerken dan is het van belang om de rolverdeling tussen partijen te duiden en afhankelijk daarvan een overeenkomst te sluiten, zoals een verwerkersovereenkomst.
Link naar de website van de AP voor meer informatie: https://www.autoriteitpersoonsgegevens.nl/

Toezicht en handhaving NL en EU

In Nederland is de toezichthouder de Autoriteit Persoonsgegegvens (AP). De AP is bevoegd om sancties op te leggen als een organisatie de privacywetgeving overtreedt. De belangrijkste sancties zijn de boete, de last onder dwangsom, het verwerkingsverbod, de berisping en de waarschuwing. Een boete is maximaal 20 miljoen euro of 4% van de wereldwijde jaaromzet. In Europa is de EDPS de toezichthoude die erop toeziet dat de Europese instellingen zelf de gegevensbeschermingsregels naleven en het behandelt klachten daarover.

Raakvlakken andere wetgeving

De DA en de Data Governance Act (DGA) versterken elkaar om betrouwbare en veilige toegang tot gegevens te vergemakkelijken en het gebruik ervan in belangrijke economische sectoren en gebieden van algemeen belang te bevorderen. De DGA regelt processen en structuren voor vrijwillige gegevensdeling, terwijl de DA bepaalt wie waarde kan creëren uit data en onder welke voorwaarden. Samen zullen deze twee wetgevingen helpen bij het creëren van een interne EU-markt voor gegevens. De verhouding tussen de Algemene Verordening Gegevensbescherming (AVG), de Data Governance Act (DGA) en de Data Act (DA) draait om gegevensregulering. Omdat alle drie wetgevingen gegevens behandelen, kan er overlap zijn tussen hen. De AVG is specifiek van toepassing op persoonsgegevens, wat betekent dat gegevens die niet direct of indirect aan individuen kunnen worden gekoppeld, buiten het toepassingsgebied vallen. De DGA en de DA zijn breder en omvatten alle soorten gegevens. Ze hanteren ruimere definities van 'gegevens', waaronder persoonsgegevens. De DGA regelt bijvoorbeeld het hergebruik van niet-publiek toegankelijke overheidsgegevens, waarin zowel bedrijfsgeheimen, intellectuele eigendomsrechten als persoonsgegevens kunnen voorkomen. De DA is van toepassing op zowel persoonsgegevens als niet-persoonsgegevens.

Hoewel alle drie de verordeningen persoonsgegevens omvatten, rijst de vraag welke voorrang heeft bij een conflict tussen hen. Zowel de DGA als de DA stellen dat de AVG prevaleert bij inconsistenties.

TOI-Vo EU-Verordening inzake het tegengaan van de verspreiding van terroristische online-inhoud (2021/784) (Regulation)	Bron http://data.europa.eu/eli/reg/2021/784/oj

Doelgroep

Aanbieders van hostingdiensten in de EU, ongeacht of ze hun hoofdvestiging in de EU-lidstaten hebben.

Van toepassing vanaf

Op 7 juni 2022 is de (EU) 2021/784 in werking getreden. Deze verordening is in Nederland geïmplementeerd in de "Uitvoeringswet verordening terroristische online-inhoud". Deze is van toepassing vanaf 1 september 2023.

Impact

Onder "terroristische inhoud" wordt verstaan het aanzetten of aansporen tot het plegen van, of tot het leveren van een bijdrage aan het plegen van, terroristische misdrijven, dat iemand aanspoort om deel te nemen aan activiteiten van een terroristische groepering, of dat terroristische activiteiten verheerlijkt, met inbegrip van materiaal waarop een terroristische aanslag wordt afgebeeld.
De definitie moet ook materiaal omvatten dat instructies geeft voor het maken of gebruiken van explosieven, vuurwapens of andere wapens of schadelijke of gevaarlijke stoffen, evenals chemische, biologische, radiologische en nucleaire stoffen (CBRN-stoffen), of voor andere specifieke methoden of technieken, met inbegrip van het selecteren van doelwitten, voor het plegen of het bijdragen aan het plegen van terroristische misdrijven. Dergelijk materiaal omvat tekst, beelden, geluidsopnamen en video's, alsmede het rechtstreeks uitzenden van terroristische misdrijven, waardoor het gevaar ontstaat dat nog meer zulke misdrijven worden gepleegd. Bij de beoordeling of materiaal terroristische inhoud in de zin van deze verordening uitmaakt, moeten bevoegde autoriteiten en aanbieders van hostingdiensten rekening houden met factoren zoals de aard en de bewoordingen van verklaringen, de context waarin de verklaringen zijn afgelegd en hun potentieel om schadelijke gevolgen voor de veiligheid en beveiliging van personen teweeg te brengen.

Aanbieders van hostingdiensten die aan terroristische inhoud worden blootgesteld, moeten in hun algemene voorwaarden — als ze die hebben — bepalingen opnemen om het misbruik van hun diensten voor de verspreiding van terroristische inhoud tegen te gaan. Zij moeten die bepalingen op een zorgvuldige, transparante, proportionele en niet-discriminerende wijze toepassen.
De aanbieder van hostingdiensten moet bij de bevoegde autoriteit verslag uitbrengen over de specifieke maatregelen zodat die bevoegde autoriteit kan beoordelen of de maatregelen doeltreffend en proportioneel zijn en of, indien automatische middelen worden gebruikt, de aanbieder van hostingdiensten over de nodige capaciteiten beschikt voor toezicht en verificatie door mensen.
Aanbieders van hostingdiensten zijn verplicht om de in het verwijderingsbevel geïdentificeerde terroristische inhoud binnen één uur na ontvangst van het verwijderingsbevel te verwijderen of de toegang daartoe in alle lidstaten te blokkeren.

Toezicht en handhaving NL en EU

De Autoriteit Online Terroristisch en Kinderpornografisch Materiaal (AOTKM) kan verwijderingsbevelen uitvaardigen, deze bevelen beoordelen, toezien op specifieke maatregelen en sancties opleggen. Deze AOTKM kan gegevens uitwisselen en onderling, en waar passend met Europol, coördineren en samenwerken. De financiële sancties opleggen, zoals een last onder dwangsom, kan oplopen tot ten hoogste 4% van de mondiale omzet van de aanbieder van hostingdiensten in het voorafgaande boekjaar.

Raakvlakken andere wetgeving

Beide verordeningen (TOI-Vo en SMK-Vo) bepalen dat aanbieders van hostingdiensten specifieke ongewenste content op verzoek van een opsporingsautoriteit binnen een bepaalde (relatief korte) termijn moeten verwijderen.

SMK-Vo Verordening ter voorkoming en bestrijding van seksueel misbruik van kinderen (Regulation)	Bron http://data.europa.eu/eli/reg/2021/1232/oj

Doelgroep

Aanbieders van hostingdiensten en aanbieders van publiek beschikbare interpersoonlijke communicatiediensten

Van toepassing vanaf

De verordening is nog niet in werking getreden. Onduidelijk is wanneer dit zal plaatsvinden.

Impact

Aanbieders van hostingdiensten en aanbieders van interpersoonlijke communicatiediensten identificeren, analyseren en beoordelen voor elke dergelijke dienst die zij aanbieden het risico dat de dienst wordt gebruikt voor online seksueel misbruik van kinderen. De term “seksueel misbruik van kinderen” dient niet alleen betrekking te hebben op de verspreiding van materiaal waarvan eerder is vastgesteld en bevestigd dat het materiaal van seksueel misbruik van kinderen is (“bekend” materiaal), maar ook van niet eerder vastgesteld materiaal dat waarschijnlijk materiaal van seksueel misbruik van kinderen is, maar dat nog niet als zodanig is bevestigd (“nieuw” materiaal), alsook op activiteiten die neerkomen op het benaderen van kinderen (“grooming”).

Aanbieders van hostingdiensten moeten een risicobeoordeling maken, risicobeperkingen doorvoeren, verder kan de opsporingsautoriteit de aanbieder van hostingdiensten verplichten maatregelen (zoals het installeren nieuwe technologieën) te nemen om seksueel misbruik op te sporen. Verder heeft de aanbieder een meldingsplicht, en een plicht om de content na een verzoek van de opsporingsautoriteit zo snel mogelijk en in ieder geval binnen 24 uur te verwijderen.

Door de oprichting van een Europees centrum ter voorkoming en bestrijding van seksueel misbruik van kinderen (“het EU-centrum”) wordt met het voorstel tevens geprobeerd om aanbieders te helpen zich van hun verantwoordelijkheden te verminderen. Het EU-centrum zal met name databanken met indicatoren van online seksueel misbruik van kinderen opzetten, onderhouden en beheren, die door de aanbieders moeten worden gebruikt om aan hun opsporingsverplichtingen te voldoen.

Toezicht en handhaving NL en EU

Het EU-centrum zal nauw samenwerken met de coördinerende autoriteit. Op dit moment is niet bekend wie in Nederland de coördinerende autoriteit wordt. De verwachting is dat dit de Autoriteit Online Terroristisch en Kinderpornografisch Materiaal (AOTKM) wordt.
De coördinerende autoriteit kan verwijderingsbevelen uitvaardigen, toezien op specifieke maatregelen en sancties opleggen. Sancties voor het verstrekken van onjuiste, onvolledige of misleidende informatie, voor het nalaten van antwoord te geven, het nalaten van onjuiste, onvolledige of misleidende informatie te rectificeren of het weigeren zich aan een inspectie ter plaatse te onderwerpen, zijn niet hoger dan 1 % van de jaarlijkse inkomsten of totale omzet van de aanbieder.
Overige financiële sancties kunnen oplopen tot ten hoogste 6% van de mondiale omzet van de aanbieder van hostingdiensten.

Raakvlakken andere wetgeving

Beide verordeningen (TOI-Vo en SMK-Vo) bepalen dat aanbieders van hostingdiensten specifieke ongewenste content op verzoek van een opsporingsautoriteit binnen een bepaalde (relatief korte) termijn moeten verwijderen.

DORA Digital Operation Resilience Act (Regulation)	Bron http://data.europa.eu/eli/reg/2022/2554/oj

Doelgroep

Financiële instellingen en bedrijven die ICT-diensten aan deze financiële instellingen verlenen. Dit omvat onder andere banken, verzekeringsmaatschappijen, handelsplatformen, beleggingsinstellingen en dienstverleners op het gebied van crypto-activa. Bovendien is de DORA van toepassing op ICT-leveranciers die diensten leveren aan financiële bedrijven, evenals op (ICT-)bedrijven die zelf financiële diensten verlenen.

Van toepassing vanaf

DORA is per 17 januari 2023 in werking getreden en is van toepassing vanaf 17 januari 2025.

Impact

DORA betreft een Europese verordening die tot doel heeft de financiële sector in de EU te versterken, veerkrachtiger te maken en IT-risico's effectiever te laten beheren tegen groeiende cyberdreigingen, zoals cyberaanvallen en datalekken.
Hoewel de DORA-verordening ruimte biedt voor gedelegeerde handelingen, oftewel verdere regelgeving op dit gebied, zijn de hoofdlijnen gedetailleerd vastgelegd. DORA omvat onder andere de volgende inhoud:

- Herziene organisatie en bestuur: binnen het kader van DORA moeten specifieke bestuurlijke en organisatorische vereisten worden nageleefd met betrekking tot het monitoren van ICT-risico's.
- Implementatie van een ICT-risk management framework: financiële entiteiten zijn verplicht om een ICT-risk management framework te implementeren als onderdeel van hun algehele risicobeheersysteem.
- ICT-incidentrapportage: er moet een specifieke procedure worden ingevoerd voor het melden van incidenten die verband houden met ICT.
- Digitale operationele weerbaarheidsstrategie: er dienen maatregelen te worden genomen om cyberincidenten te voorkomen, te ontdekken, de schade te beperken en een snel herstel te waarborgen.
- Toezicht op ICT-risicobeheer bij derde partijen: conform DORA zijn financiële entiteiten verantwoordelijk voor de ICT-risico's van derde partijen, waarbij ze deze risico's moeten definiëren en nauwlettend moeten monitoren.

Toezicht en handhaving NL en EU

De Europese Toezichthoudende Autoriteiten (ETA's) kunnen samen met relevante autoriteiten, de ECB en het ESRB, mechanismen introduceren om het delen van praktijken tussen financiële sectoren te bevorderen en cyberkwetsbaarheden aan te pakken.
De ETA's dienen de vereisten uit te werken waaraan moet worden voldaan. Dit wordt onder andere gedaan door middel van Regulatory Technical Standards (RTS'en) en Joint Guidelines.
Er zijn in totaal 10 van deze standaarden uitgegeven in twee groepen voor publieke consultatie, en recentelijk zijn de eerste 4 definitief vastgesteld.
De link naar deze eerste 4 documenten is: https://www.eiopa.europa.eu/publications/set-rules-under-dora-ict-and-third-party-risk-management-and-incident-classification_en

De ETA's kunnen ook crisisoefeningen ontwikkelen voor een gecoördineerde EU-respons op ernstige cyberaanvallen. Daarnaast werken de ETA's nauw samen om toezicht te coördineren, goede praktijken te bevorderen en inbreuken op regelgeving aan te pakken.

In Nederland is De Nederlandsche Bank verantwoordelijk gesteld voor het toezicht. Diverse maatregelen, waaronder boetes, tijdelijke opschorting van diensten en intrekking van vergunningen, kunnen worden toegepast als sancties. De boetes voor individuele instellingen kunnen oplopen tot 1 procent van hun wereldwijde omzet.

Raakvlakken andere wetgeving

DORA fungeert als een aanvullende maatregel op bestaande wetgeving, waaronder NIS2 en AVG, met betrekking tot financiële instellingen en bedrijven aanverwante ICT-diensten leveren.

CSA (EU) 2023/0109 Cyber Solidarity Act (Regulation)	Bron https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52023PC0209

Doelgroep

Entiteiten die actief zijn in zeer kritieke sectoren (gezondheidszorg, transport, energie, enz.) kunnen worden onderworpen aan zogenaamde 'gecoördineerde paraatheidstests'. Daarnaast is het mogelijk om deel te nemen aan de EU-Cyberbeveiligingsreserve.

Van toepassing vanaf

De CSA (EU) 2023/0109 is nog niet in werking getreden. Onduidelijk is wanneer dit zal plaatsvinden.

Impact

Het doel van deze verordening is het versterken van de capaciteit binnen de EU om belangrijke en omvangrijke cyberbedreigingen en -aanvallen te detecteren, voor te bereiden en erop te reageren. Het voorstel omvat de oprichting van een Europees cyberbeveiligingsschild, bestaande uit onderling verbonden operationele beveiligingscentra door de EU, en een alomvattend noodmechanisme voor cyberbeveiliging om de cyberveerkracht van de EU te verbeteren. Het Europees cyberschild zal worden opgebouwd uit veiligheidsoperatiecentra (SOC's) verspreid over de gehele EU, gegroepeerd in diverse SOC-platforms met meerdere landen, gefinancierd met steun van het Digitaal Europa-programma (DEP) naast nationale financiering. Het Cyber Shield zal verantwoordelijk zijn voor het verbeteren van de detectie, analyse en respons op cyberdreigingen. Deze SOC's zullen geavanceerde technologieën zoals kunstmatige intelligentie (AI) en gegevensanalyse inzetten om waarschuwingen voor dergelijke bedreigingen te detecteren en te delen met autoriteiten over grenzen heen. Het cybernoodmechanisme heeft tot doel de paraatheid en respons op cyberincidenten te verbeteren door middel van drie hoofdacties:

- Het testen van cruciale sectoren (zoals zorg, transport en energie) op mogelijke zwakke punten in hun cyberbeveiliging, gebaseerd op een gemeenschappelijke risicobeoordeling op EU-niveau.
- De oprichting van een EU-cyberbeveiligingsreserve, bestaande uit incidentresponsdiensten van particuliere dienstverleners, die op verzoek van lidstaten of EU-instellingen kunnen worden ingezet bij de aanpak van significante of grootschalige cyberbeveiligingsincidenten.
- Het bieden van wederzijdse bijstand tussen lidstaten om elkaar te ondersteunen bij de aanpak van cyberbeveiligingsincidenten.

De voorgestelde verordening omvat ook het instellen van een mechanisme voor de evaluatie van cyberbeveiligingsincidenten, met als doel specifieke incidenten te beoordelen en te evalueren. Op verzoek van de Commissie of nationale autoriteiten (het EU-CyCLONe-netwerk of het CSIRT-netwerk) zal ENISA ten aanzien van cyberbeveiliging verantwoordelijk zijn voor het beoordelen van specifieke significante of grootschalige cyberbeveiligingsincidenten. ENISA moet een rapport opstellen met lessen en, indien van toepassing, aanbevelingen ter verbetering van de cyberrespons van de EU.

Toezicht en handhaving NL en EU

Niet van toepassing.

Raakvlakken andere wetgeving

De CSA (EU) 2023/0109 vult structuren aan en ondersteunt die in het kader van andere cyberbeveiligingsinstrumenten, zoals NIS2-richtlijn of CSA (EU) 2019/881. Deze aanvulling en ondersteuning bestaat uit het nemen van doeltreffende maatregelen en loyaal, efficiënt, solidair en gecoördineerd met elkaar, de Commissie en andere relevante overheidsinstanties alsook de betrokken entiteiten samen te werken om kritieke infrastructuur die wordt gebruikt om essentiële diensten op de interne markt te verlenen weerbaarder te maken.

CSA (EU) 2019/881 Cybersecurity Act (Regulation)	Bron http://data.europa.eu/eli/reg/2019/881/oj

Doelgroep

De CSA is in de eerste plaats van toepassing op alle ICT-producten, ICT-diensten en ICT-processen, en de fabrikanten of aanbieders ervan, voor zover relevant. Een ICT-product verwijst naar een "element of groep elementen van een netwerk- of informatiesysteem", zoals een IoT-hardware of softwarepakket. Een ICT-dienst is een "dienst die volledig of hoofdzakelijk bestaat uit de verzending, opslag, opvraging of verwerking van gegevens door middel van netwerk- en informatiesystemen". Een ICT-proces wordt beschreven als een "reeks activiteiten die worden uitgevoerd om een ICT-product of ICT-dienst te ontwerpen, ontwikkelen, leveren of onderhouden".

Van toepassing vanaf

De CSA (EU) 2019/881 is op 27 juni 2019 in werking getreden. De meeste regels zijn vanaf 28 juni 2021 van toepassing. Inmiddels zijn alle regels van toepassing.

Impact

De CSA heeft als voornaamste doel de cyberbeveiliging in Europa te verbeteren door middel van het vaststellen van technische eisen, normen en procedures voor ICT-producten, -diensten en -processen. Fabrikanten en aanbieders hebben aanvankelijk de mogelijkheid om op vrijwillige basis te kiezen voor certificering op het gebied van cyberbeveiliging of voor een EU-conformiteitsverklaring. Echter, andere EU-wetgeving, zoals de NIS2-richtlijn, kan certificering onder de Cybersecurity Act voorschrijven.
De CSA definieert drie mogelijke zekerheidsniveaus, afhankelijk van de kans op en de gevolgen van een incident met betrekking tot een ICT-product, -dienst of -proces tijdens het beoogde gebruik ervan. Deze niveaus zijn bedoeld om aan te geven hoe goed een product, dienst of proces beschermd zou moeten zijn tegen cyberaanvallen, waarbij hogere niveaus meer bescherming bieden.

Naast het vaststellen van deze certificeringsregelingen, versterkt de CSA ook het mandaat van ENISA, het Agentschap van de Europese Unie voor cyberbeveiliging. ENISA krijgt een belangrijke rol als Europees agentschap voor cyberbeveiliging en zal in opdracht van de Europese Commissie certificeringsregelingen ontwikkelen. Deze regelingen, ook wel certificeringsschema's genoemd, worden overgedragen aan de Europese Commissie, die ze vervolgens omzet in Europese regelgeving.
Inbreuken op Europese cyberbeveiligingscertificeringsregelingen worden gesanctioneerd onder nationaal recht. Dit zorgt voor een adequaat juridisch kader om naleving te waarborgen en eventuele overtredingen te bestraffen, waardoor de effectiviteit van de certificeringsregelingen wordt versterkt en de cyberbeveiliging in Europa wordt verbeterd.
Link naar ENISA: https://www.enisa.europa.eu/topics/certification/?tab=details

Toezicht en handhaving NL en EU

De CSA vereist dat elke EU-lidstaat ten minste één National Cybersecurity Certification Authority (NCCA) aanwijst. In Nederland wordt de rol van NCCA vervuld door de Rijksinspectie Digitale Infrastructuur, die deel uitmaakt van het ministerie van Economische Zaken en Klimaat. In Nederland is de EU Cybersecurity Act geïmplementeerd via de Uitvoeringswet Cyberbeveiligingsverordening, waarbij aanvullende bepalingen voor zekerheidsniveau 'hoog' en handhaving zijn opgenomen. Overtredingen kunnen leiden tot maatregelen door de Minister, boetes, dwangsommen of intrekking van de certificering.

Raakvlakken andere wetgeving

De door ENISA ontworpen certificeringsschema's worden gebaseerd op ontwerpen die zijn voorbereid door in nauwe samenwerking met experts uit de industrie en lidstaten, na technische en juridische discussies, evenals een openbare raadpleging. De schema's zullen de Cyber Resilience Act aanvullen die bindende cybersecurity-eisen introduceert voor alle hardware- en softwareproducten in de EU. Deze belangrijke stap draagt bij aan het bevorderen van het mondiale digitale leiderschap van Europa. Certificering in overeenstemming met de schema's van de CSA is vrijwillig, maar kan verplicht gesteld worden in het kader van NIS2.

CSRD Corporate Sustainability Reporting Directive (Directive)	Bron http://data.europa.eu/eli/dir/2022/2464/oj

Doelgroep

De CSRD-regeling is van toepassing op verschillende categorieën ondernemingen, namelijk (a) grote ondernemingen en grote groepen, (b) middelgrote of kleine beursondernemingen, en (c) bepaalde niet-EU ondernemingen.

A. Een grote onderneming volgens de CSRD is kortweg gedefinieerd als een onderneming die op twee opeenvolgende balansdata aan minstens twee van de volgende drie criteria voldoet:
   - Een balanstotaal van meer dan € 20.000.000,-;
   - Een netto-omzet van meer dan € 40.000.000,-; en/of
   - Op jaarbasis een gemiddeld personeelsbestand van meer dan 250.

Een grote groep omvat een moederonderneming en één of meerdere dochtervennootschappen waar de moeder zeggenschap over heeft, en waarbij de groep als geheel op twee opeenvolgende balansdata aan minstens twee van de bovengenoemde drie criteria voldoet.

B. Middelgrote of kleine beursondernemingen onder de CSRD zijn ondernemingen waarvan de effecten (zoals aandelen en obligaties) op een Europese beurs worden verhandeld en die groter zijn dan micro-ondernemingen. Micro-ondernemingen voldoen aan minstens twee van de volgende drie criteria:
   - Een balanstotaal gelijk aan of minder dan € 350.000,-;
   - Een netto-omzet gelijk aan of minder dan € 700.000,-; en/of
   - Op jaarbasis een gemiddeld personeelsbestand gelijk aan of minder dan 10.

C. De CSRD-regels zijn van toepassing op ondernemingen opgericht naar of beheerst door het recht van een EU-lidstaat. Er is een poging gedaan om onder bepaalde omstandigheden ook ondernemingen opgericht naar of beheerst door het recht van een niet-EU-lidstaat (indirect) onder de CSRD te laten vallen. Dit geldt als er binnen de EU een dochteronderneming of bijkantoor bestaat en/of aan specifieke omzeteisen wordt voldaan.

Ondernemingen uit derde landen met aanzienlijke activiteiten op het grondgebied van de EU worden verplicht om direct of via hun EU-dochteronderneming of bijkantoor een duurzaamheidsverslag te publiceren, met name over de effecten van hun activiteiten op sociale en milieukwesties. Hoewel er enkele vrijstellingen bestaan voor de inhoud van het duurzaamheidsverslag, worden dergelijke ondernemingen uit derde landen op deze manier ook aansprakelijk gehouden voor de impact die zij hebben op mens en milieu.

Van toepassing vanaf

In werking getreden op 5 januari 2023. Van toepassing op grote organisaties van openbaar belang (banken, verzekeraars, beursvennootschappen) op boekjaren startend op of vanaf: 1 januari 2024.
Van toepassing op grote ondernemingen en groepen op boekjaren startend op of vanaf: 1 januari 2025.
Van toepassing middelgrote of kleine beursondernemingen en groepen op boekjaren startend op of vanaf: 1 januari 2026.
Van toepassing op bepaalde niet-EU-ondernemingen middelgrote of kleine beursondernemingen en groepen op boekjaren startend op of vanaf: 1 januari 2028.
Eerste conform CSRD opgestelde duurzaamheidsverslag moet worden gepubliceerd in kalenderjaar na jaar van toepassingverklaring.

Impact

Bedrijven die onder het toepassingsbereik vallen dienen verplicht verslag uit te brengen over hun prestaties op het gebied van duurzaamheid. Duurzaamheidsverslaggeving is één van de hoekstenen van de Europese Green Deal en de Sustainable Finance Agenda én maakt deel uit van een breder beleid van de Europese Unie om ondernemingen te verplichten mensenrechten te respecteren en hun impact op de planeet te verminderen. Het hoofddoel van deze regelgeving is om investeerders en consumenten in staat te stellen weloverwogen duurzame keuzes te maken.

De CSRD (Corporate Sustainability Reporting Directive) specificeert gedetailleerd welke informatie moet worden opgenomen in het verslag van een onderneming. Het verslag moet onderscheid maken tussen korte-, middellange- en langetermijnaspecten. Belangrijke elementen die moeten worden beschreven, omvatten het bedrijfsmodel en de strategie, met aandacht voor veerkracht en kansen op het gebied van duurzaamheid. Verder dienen toekomst- en investeringsplannen te worden gepresenteerd, gericht op de verenigbaarheid met een duurzame economie en het Parijse Klimaatakkoord.

Andere vereisten omvatten het vermelden van tijdgebonden duurzaamheidsdoelen, de voortgang en de wetenschappelijke basis ervan. De rol van bestuursorganen met betrekking tot duurzaamheidskwesties, hun expertise en eventuele stimuleringsregelingen moeten worden belicht, samen met het duurzaamheidsbeleid van de onderneming en toegepaste zorgvuldigheidsprocedures. Negatieve effecten van eigen activiteiten en de keten moeten worden beschreven, inclusief genomen maatregelen en resultaten. Voor clouddienstverleners is dit van belang vanwege de aard van hun activiteiten. Zij verbruiken aanzienlijke hoeveelheden energie vanwege de constante werking van datacenters die nodig zijn om de diensten te ondersteunen, zeker wanneer er (ook) gebruik wordt gemaakt van kunstmatige intelligentie.. Belangrijkste risico's met betrekking tot duurzaamheid en beheersmaatregelen, evenals relevante indicatoren, moeten ook worden gerapporteerd.
Ondernemingen moeten tevens verklaren hoe ze de benodigde informatie hebben verzameld op al deze gebieden om aan de CSRD te voldoen.
Daarnaast is er sprake van een verplichte 'limited assurance', waarbij een externe accountantscontrole noodzakelijk is om de betrouwbaarheid van de gerapporteerde informatie te waarborgen. Deze maatregelen zijn bedoeld om bedrijven aan te moedigen verantwoordelijkheid te nemen voor hun duurzaamheidsprestaties en tegelijkertijd het bewustzijn en de besluitvorming van investeerders en consumenten te verbeteren.

Toezicht en handhaving NL en EU

De verwachting is dat de nationale implementatie van de CSRD zal plaatsvinden door wijzigingen in bestaande wetgeving, zoals de Wet op het financieel toezicht, de Wet toezicht accountantsorganisaties, de Wet op het accountantsberoep, het Burgerlijk Wetboek en de Wet tuchtrechtspraak accountants.De Nederlandse wetgever moet nog specifieke sancties bepalen bij overtreding van de verplichtingen inzake duurzaamheidsrapportages. Verwacht wordt dat naast financiële sancties het overtreden van de verplichtingen inzake duurzaamheidsrapportages leidt tot reputatieschade.

Raakvlakken andere wetgeving

CSRD draait om het rapporteren van duurzaamheidsinspanningen, terwijl CSRDDD zich richt op het actief identificeren, voorkomen en verminderen van actuele risico's in de toeleveringsketen.

CSDDD Corporate Sustainability Due Diligence Directive (Directive)	Bron https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0071

Doelgroep

De CSDDD is van toepassing op ondernemingen met meer dan 1000 werknemers en een wereldwijde omzet van meer dan EUR 450 miljoen. De CSDDD is ook van toepassing op ondernemingen met een wereldwijde omzet van meer dan EUR 80 miljoen die via franchise- of licentieovereenkomsten meer dan EUR 22,5 miljoen aan royalty's in de EU genereren, onder voorwaarde van een gezamenlijke identiteit, businessconcept en uniforme businessmethoden.

De implementatie wordt gefaseerd uitgevoerd met termijnen voor verschillende grootte van ondernemingen:
- Meer dan 5000 werknemers en een netto omzet van EUR 1.500 miljoen moeten voldoen tegen 2027.
- Meer dan 3000 werknemers en een netto-omzet van EUR 900 miljoen moeten voldoen tegen 2028.
- Meer dan 1000 werknemers en een netto-omzet van EUR 300 miljoen moeten voldoen tegen 2029."

Van toepassing vanaf

Op 24 april 2024 heeft het Europees Parlement de CSDDD goedgekeurd. De CSDDD moet nu formeel worden aangenomen door de Europese Raad om van kracht te worden. Naar verwachting zal de CSDDD eind mei 2024 worden gepubliceerd. Twintig dagen daarna zal de CSDDD inwerkingtreden. Vanaf dat moment hebben lidstaten twee jaar de tijd om de CSDDD te implementeren in nationale wetgeving.

Impact

De voorgestelde CSDDD (Corporate Sustainability Due Diligence Directive) stelt grote ondernemingen verplicht om voortdurend onderzoek te doen naar zowel hun eigen bedrijfsactiviteiten als die van hun vaste samenwerkingspartners. Hierbij dienen zij de effecten van deze activiteiten op zowel het milieu als de mensenrechten te identificeren.

Indien de bedrijfsactiviteiten van de ondernemingen negatieve gevolgen hebben voor het milieu en de mensenrechten, zijn zij verplicht passende maatregelen te treffen om deze negatieve effecten te voorkomen, verminderen en beëindigen. De kans is groot dat dit voor clouddienstverleners (zeker als zij kunstmatige intelligentie ontwikkelen, gebruiken of verkopen) grote impact gaat hebben.

Jaarlijks moeten ondernemingen verplicht monitoren of hun eigen beleid inzake due diligence en de genomen maatregelen effectief zijn.

Daarnaast dienen zij een klachtenprocedure in te richten, waardoor burgers, maatschappelijke organisaties en vakbonden die te maken hebben met negatieve effecten, hun bezwaren kenbaar kunnen maken.

De CSDDD omvat clausule die gedetailleerd beschrijft hoe bedrijven op een substantiële manier hun belanghebbenden moeten betrekken. In essentie vereist dit dat belanghebbenden worden geraadpleegd voor:
-Het verkrijgen van informatie over mogelijke en feitelijke negatieve effecten.
-Het opstellen van een preventief of corrigerend actieplan.
-Het nemen van beslissingen over het beëindigen van zakelijke relaties.
-Het implementeren van passende maatregelen.

-Indien van toepassing, het ontwikkelen van kwalitatieve en kwantitatieve indicatoren voor het monitoren van de due diligence activiteiten.

Tenslotte zijn ondernemingen verplicht om publiekelijk te communiceren over hun due diligence beleid en de getroffen maatregelen.

De verwachting is dat de implementatie van de CSDDD aanzienlijke invloed zal hebben op de bedrijfsvoering van grote ondernemingen. Na de inwerkingtreding dienen zij continu due diligence onderzoek te verrichten en passende maatregelen te nemen om negatieve effecten van hun bedrijfsvoering te voorkomen, verminderen en beëindigen.

Toezicht en handhaving NL en EU

Het is momenteel nog onduidelijk welke toezichthouder in Nederland wordt aangewezen voor de toezicht en handhaving ten aanzien van de CSDDD.
De toezichthoudende autoriteit heeft de bevoegdheid om op eigen initiatief of naar aanleiding van gemotiveerde bezwaren een onderzoek te openen als ze voldoende informatie heeft over mogelijke inbreuken door een bedrijf op nationale wetgeving die voortvloeit uit een specifieke richtlijn. Als de autoriteit vaststelt dat deze nationale bepalingen niet worden nageleefd, moet het betrokken bedrijf binnen een redelijke termijn corrigerende maatregelen nemen. Het nemen van corrigerende maatregelen sluit echter niet uit dat administratieve sancties kunnen worden opgelegd of dat wettelijke aansprakelijkheid ontstaat in geval van schade. De toezichthoudende autoriteiten hebben minimaal de bevoegdheid om te eisen dat overtredingen worden beëindigd, herhaling wordt voorkomen en passende herstelmaatregelen worden genomen. Ze kunnen ook geldboetes opleggen en tussentijdse maatregelen nemen om ernstige en onherstelbare schade te voorkomen. Wanneer geldboetes worden opgelegd, worden deze gebaseerd op de omzet van de onderneming. De sancties die worden opgelegd moeten publiekelijk worden bekendgemaakt.

Raakvlakken andere wetgeving

CSRD draait om het rapporteren van duurzaamheidsinspanningen, terwijl CSRDDD zich richt op het actief identificeren, voorkomen en verminderen van actuele risico's in de toeleveringsketen.

eIDAS (1.0 en 2.0) Electronic Identification and Trust Services (Regulation)	Bron http://data.europa.eu/eli/reg/2014/910/oj https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX%3A52021PC0281

Doelgroep

Overheden en vertrouwensdienstverleners

Van toepassing vanaf

eIDAS 1.0 al geldt sinds 29 september 2018 en op het moment van schrijven wordt er onderhandeld over wijziging van de verordening (eIDAS 2.0). De datum waarop eIDAS 2.0 van kracht wordt is nog niet bekend.

Impact

De huidige eIDAS-verordening (1.0) stelt uniforme eisen aan de betrouwbaarheidsniveaus van elektronische ID's. Daarnaast biedt het een kader voor verschillende soorten elektronische handtekeningen, waaronder de gewone, geavanceerde en gekwalificeerde elektronische handtekening. Het gebruik van elektronische handtekeningen vereist een analyse van het vereiste type handtekening en de geschiktheid ervan voor de beoogde transacties.

De nieuwe eIDAS-verordening (2.0) biedt alle burgers in de EU een digitale identiteit die gebruikers in staat stellen om zich hiermee online en offline grensoverschrijdend te identificeren en te authentiseren om toegang tot een breed scala openbare en particuliere diensten te krijgen.
De overeenstemming van de Europese portemonnees voor digitale identiteit met die vereisten moet worden gecertificeerd door de lidstaten aangewezen geaccrediteerde openbare of private organen. Het gebruik van een certificeringsregeling op basis van met de lidstaten overeengekomen beschikbare gemeenschappelijke normen moet een hoog niveau van vertrouwen en interoperabiliteit waarborgen. Certificering moet met name steunen op de NIS2-richtlijn.
Deze portemonnee biedt een optionele digitale identiteit waarmee individuen controle hebben over hun persoonlijke gegevens. Het kan worden gebruikt als een identificatiemiddel om specifieke documenten te verstrekken. Enkele voorbeelden van het gebruik van deze portemonnee zijn: toegang krijgen tot een persoonlijke bankrekening of het aanvragen van een lening; het indienen van belastingaangiften en het voltooien van inschrijvingen bij onderwijsinstellingen.
Decentrale overheden zullen verplicht zijn om de Europese digitale identiteit te erkennen zodra de bijbehorende verordening van kracht wordt. Dit betekent dat zij moeten zorgen voor de integratie van de genoemde middelen, zoals de digitale wallet, en nieuwe vertrouwensdiensten in hun dienstverlening, inclusief het verstrekken van benodigde ondersteuning.

Toezicht en handhaving NL en EU

Toezicht op eIDAS 1.0 is geregeld in de Telecomwet. De toezichthouder is de Rijksinspectie Digitale Infrastructuur, wat valt onder het Ministerie van Economische Zaken en Klimaat. De verwachting is dat de nieuwe verordening hier ook onder gaat vallen.

Raakvlakken andere wetgeving

Niet van toepassing.