Onderzoek impact EU-regelgeving op OCW-beleidsterreinen

Eindrapport

Dialogic
Melvin Hanswijk
Max Boiten

Opdrachtgever: Ministerie van Onderwijs, Cultuur en Wetenschap
Publicatienummer: 2022.104.2237
Datum: 20-10-2022

Scope en inhoud onderzoek

Aanleiding en doel van het onderzoek

- De Europese Commissie heeft de afgelopen jaren een groot aantal wetgevingsvoorstellen gepubliceerd op het gebied van digitalisering en data. Binnen het ministerie van OCW is er een brede behoefte aan overzicht met betrekking tot de relevantie van deze EU-regels voor de OCW-beleidsterreinen. Een dergelijk overzicht kan als basis dienen voor de toekomstige OCW-inzet, ook in relatie tot nationale uitvoeringsmaatregelen.
- Het doel van dit onderzoek is om een breed overzicht te geven van elf stukken voorgestelde regelgeving. Het doel is niet om de diepte in te gaan. Op basis van de bevindingen van dit onderzoek kan worden besloten waar meer aandacht aan moet worden besteed.

Inhoud

- In dit slidedeck behandelen we elf stukken regelgeving, geselecteerd door OCW, waarbij het volgende aan bod komt:
  - De inhoud van het voorstel
  - De fase waarin het voorstel zich bevindt
  - De relatie van het voorstel tot andere regelgeving
  - De relevantie van het voorstel voor de beleidsterreinen van OCW
- Specifieke aandachtspunten worden in een apart hoofdstuk verder toegelicht.
- Wat betreft de inhoud van de voorstellen wordt telkens in een of enkele slides een overzicht gegeven van de rechten en plichten die een voorstel bevat en de doelgroepen waarop zij betrekking hebben. Deze overzichten zijn noodzakelijkerwijs niet uitputtend, maar zijn opgesteld om een zo goed mogelijk beeld te geven van de inhoud van de regeling. Het detailniveau van de overzichten is afhankelijk van de omvang, het detailniveau en de verwachte relevantie van de betreffende regeling.

Overzicht bestudeerde regelgeving

DIGITALE DIENSTEN EN MARKTEN

Digital Services Act (DSA)
IWT verwacht 2022

Digital Markets Act (DMA)
IWT verwacht in okt/nov 2022

Artificial Intelligence Act (AI Act)
In onderhandeling

CYBERVEILIGHEID

Cyber Security Act (CSA)
IWT 27 juni 2019

Cyber Resilience Act (CRA)
In onderhandeling

Network and Information Security Directive (NIS2)
IWT verwacht eind 2022

REGELGEVING M.B.T. DATA

Open Data Directive (ODD)
IWT 16 juli 2019

Data Governance Act (DGA)
IWT 23 juni 2022

Data Act (DA)
In onderhandeling

DIGITALE TOEKOMST

Framework European Digital Identity (EDI)
In onderhandeling

Beleidsagenda Digital Decade
In onderhandeling

dialogic
innovatie • interactie

Digitale Diensten en Markten

DSA - DMA

Digital Service Act (DSA)

Kern van de regeling

- Met de DSA wordt de regelgeving met betrekking tot digitale diensten geüpdatet. Het gaat hierbij met name om het tegengaan van illegale inhoud en het beschermen van de vrijheid van meningsuiting.
- De DSA heeft betrekking op 'tussenhandelsdiensten' (*intermediary services)*, in het kort zijn dat de partijen tússen degene die bepaalde inhoud online zet en degene die die inhoud te zien krijgt. Dit is een breed begrip, dat onder meer internetaanbieders, aanbieders van opslagruimte en sociale mediaplatformen omvat.
- De DSA sluit tussenhandelsdiensten in principe uit van (civiele en strafrechtelijke) aansprakelijkheid voor eventuele illegale inhoud, onder voorwaarde dat zij geen kennis hebben van die inhoud. Aan de tussenhandelsdiensten worden wel verschillende regels opgelegd om illegale inhoud tegen te gaan.

Verwachte impact

- Verwachte impact OCW: **KLEIN**
- Verwachte impact veld: **MEDIUM**
  - Cultuur: mogelijk veel administratieve lasten voor sommige instellingen die tussenhandelsdiensten aanbieden
  - Onderwijs: mogelijk veel administratieve lasten voor instellingen die tussenhandelsdiensten aanbieden of contractueel verplichtingen opgelegd krijgen
  - Onderzoek en wetenschap: mogelijk veel administratieve lasten voor diensten die tussenhandelsdiensten aanbieden.

Mogelijke vervolgacties

- Besteed aandacht aan de vraag of en wanneer diensten van onderwijs- en onderzoeksorganisaties ook aangemerkt kunnen worden als tussenhandelsdiensten. Zie hiervoor aandachtspunt 1.

DSA

De DSA wordt op het moment van schrijven getekend.
Inwerkingtreding wordt daarmee verwacht in 2022.
De wet wordt rechtstreeks van toepassing in de periode 2023-2024.

Fase 1 OPSTELLEN VOORSTEL

Fase 2 VOORSTEL IN ONDERHANDELING

Fase 3 INWERKINGTREDING

dialogic innovatie • interactie

DSA – relatie tot andere regelgeving

- De DSA bouwt voort op de richtlijn inzake elektronische handel. De uitsluiting van aansprakelijkheid die in die richtlijn is opgenomen, wordt met de DSA uit die richtlijn gehaald en direct in de DSA opgenomen.
- De DSA is een verordening en heeft dus directe werking.
- De DSA is lex generalis en vult sectorspecifieke wetgeving aan. Lex specialis zoals de AVMSD (mediarichtlijn) blijft van toepassing en gaat voor, de DSA heeft daar geen invloed op.
- De DSA wordt vaak samen genoemd met de Digital Markets Act (DMA), zij vormen samen het Digital Services Package. Waar de DSA gaat over het bestrijden van illegale inhoud, gaat de DMA over het bevorderen van eerlijke concurrentie in de digitale interne markt.

DSA – rechten en plichten

Doelgroep

- De regels zijn van toepassing op tussenhandelsdiensten. Er zijn drie hoofdcategorieën:
  - Mere conduit-diensten (doorgeefluik, bijvoorbeeld internetaanbieders)
  - Caching-diensten (bijvoorbeeld content delivery netwerken)
  - Hosting-diensten (bijvoorbeeld aanbieders van opslagruimte en sociale medianetwerken)
    - Subset: online platforms
      - Subset: very large online platforms (VLOPs)
- Bepaalde regels worden opgelegd aan alle tussenhandelsdiensten.
  - Er gelden extra regels voor hostingdiensten.
    - Extra regels voor de subset onlineplatforms.
      - Extra regels voor de subset zeer grote online platforms.
- Kleine ondernemingen* zijn uitgezonderd van een aantal bepalingen.
- Het is onduidelijk of diensten in het kader van onderwijs en onderzoek juridisch ook als tussenhandelsdienst kunnen kwalificeren. Uit verschillende bepalingen blijkt namelijk dat de verordening is geschreven met economische activiteiten in het hoofd, maar in de daadwerkelijke definities van (o.a.) tussenhandelsdiensten en hostingdiensten is dit niet als criterium opgenomen.**

Juridische definities (art. 2(f) en 2(h) DSA)

"tussenhandelsdienst": een van de volgende diensten:

- *een "mere conduit"-dienst die bestaat in het doorgeven in een communicatienetwerk van door een afnemer van de dienst verstrekte informatie, of in het verstrekken van toegang tot een communicatienetwerk;*
- *een "caching"-dienst die bestaat in het doorgeven in een communicatienetwerk van door een afnemer van de dienst verstrekte informatie, waarbij die informatie automatisch, tussentijds en tijdelijk wordt opgeslagen met als enige doel om de latere doorgifte van die informatie aan andere afnemers van de dienst op hun verzoek doeltreffender te maken;*
- *een "hosting"-dienst die bestaat in de opslag van de door een afnemer van de dienst verstrekte informatie, op diens verzoek;*

"onlineplatform": een aanbieder van een hostingdienst die, op verzoek van een afnemer van de dienst, informatie opslaat en verspreidt bij het publiek, tenzij […]

*Een kleine onderneming is een onderneming met minder dan 50 werknemers, waarvan de jaaromzet of het jaarlijkse balanstotaal 10 miljoen EUR niet overschrijdt. Als onderneming wordt beschouwd iedere eenheid, ongeacht haar rechtsvorm, die een economische activiteit uitoefent.

**Zie bijvoorbeeld overweging (5): "Deze verordening moet van toepassing zijn op aanbieders van bepaalde diensten van de informatiemaatschappij zoals gedefinieerd in Richtlijn (EU) 2015/1535 van het Europees Parlement en de Raad, dat wil zeggen elke dienst die gewoonlijk tegen vergoeding, langs elektronische weg, op afstand en op individueel verzoek van een afnemer wordt verricht."

DSA – rechten en plichten

Regels m.b.t. alle tussenhandelsdiensten

- Er worden eisen gesteld aan algemene voorwaarden; er moet een vast contactpunt voor autoriteiten worden aangesteld; er moet een juridisch vertegenwoordiger in de EU worden aangesteld.*
- Diensten moeten jaarlijks rapporteren over de door hen verrichte inhoudsmoderatie. (N.v.t. op kleine ondernemingen.)

Regels m.b.t. hostingdiensten

- Instellen van kennis- en actiemechanismen
  - Men moet op elektronische en gebruiksvriendelijke manier een melding van illegale inhoud kunnen maken en daarbij alle relevante informatie kunnen verstrekken.
  - De dienst moet zorgen voor tijdige, zorgvuldige en objectieve besluitvorming.
  - De dienst moet de melder onverwijld op de hoogte stellen van het besluit.
- Motivering over moderatie
  - Bij verwijderen van inhoud of het afsluiten van een afnemer informeert de instelling die afnemer.
  - De instelling motiveert hierbij ook juridisch waarom de inhoud illegaal is of in strijd is met de algemene voorwaarden.

Regels m.b.t. onlineplatforms (n.v.t. op kleine ondernemingen)

- Platforms moeten een intern klachtenafhandelingssysteem inrichten zodat afnemers bezwaar kunnen maken tegen bepaalde besluiten.
- Meldingen door 'betrouwbare flaggers'** moeten 'prioritair en onmiddellijk' worden verwerkt en afgehandeld.
- Platforms moeten meewerken aan buitengerechtelijke geschilbeslechting.
- Platforms moeten de dienstverlening opschorten indien een afnemer frequent illegale inhoud verstrekt of indien een afnemer regelmatig ongegronde meldingen maakt of ongegronde klachten indient.
- Bij een vermoeden van een ernstig strafbaar feit stellen platforms de overheid op de hoogte.
- Voor platforms waarop consumenten overeenkomsten met handelaren kunnen sluiten geldt een know-your-customer-verplichting m.b.t. de handelaren.
- Platforms moeten transparant zijn over reclame op online-interfaces.

*Er moet een juridisch vertegenwoordiger in de EU worden aangesteld indien de aanbieder niet in de EU is gevestigd.

**De status van betrouwbare flagger wordt door de overheid onder voorwaarden aan entiteiten toegekend. Zij moeten onder meer aantonen de juiste expertise te hebben, collectieve belangen te vertegenwoordigen en onafhankelijk te zijn van enig onlineplatform.

DSA – Relevantie voor de OCW-beleidsterreinen

De DSA betreft generieke regelgeving en er zijn geen sectorale uitzonderingen.

Cultuur

- Voor de mediasector is de mediarichtlijn leidend. DSA-bepalingen kunnen daarop aanvullen. Voor zover de mediarichtlijn niet anders bepaalt, zal de NPO in het kader van NPO Start moeten voldoen aan de eisen voor onlineplatforms. Vermoedelijk wordt hier al voor een groot deel aan voldaan.
- Voor de verdere cultuursector is relevant dat diensten waar bijvoorbeeld digitaal erfgoed door gebruikers wordt geüpload als hostingdienst zullen kwalificeren. Ook zullen discussiefora als onlineplatform kunnen kwalificeren en aan de betreffende regels moeten voldoen.
- De DSA zal geen harde beperkingen opleveren, maar kan (afhankelijk van de dienst) significante administratieve lasten meebrengen.

Onderwijs

- Op alle onderwijsniveaus wordt gebruik gemaakt van diensten die onder de DSA mogelijk kwalificeren als hostingdiensten en/of onlineplatforms, zoals digitale leeromgevingen. Op basis van dit onderzoek kunnen wij echter niet met zekerheid concluderen of de DSA op deze diensten van toepassing is of niet. Dit is een kwestie van juridische interpretatie. Wij bevelen OCW aan om hier nader aandacht aan te besteden en duidelijkheid over te verkrijgen. Zie ook aandachtspunt 1.
- Indien deze diensten als hostingdienst en/of onlineplatform kwalificeren kan dit leiden tot significante administratieve lasten voor onderwijsinstellingen. Dit is niet alleen van toepassing als de instelling zelf de dienst levert, maar kan ook spelen als de instelling contractueel bepaalde verantwoordelijkheden richting de leverancier krijgt. Zie ook aandachtspunt 2.

Onderzoek en Wetenschap

- Voor het onderzoeksdomein zijn het voornamelijk repositories die als hostingdienst en/of onlineplatform kunnen kwalificeren. Hierbij geldt dezelfde onzekerheid als voor diensten van onderwijsinstellingen, zie aandachtspunt 1, en spelen vergelijkbare mogelijke administratieve lasten, zie aandachtspunt 2.
- Voor specifiek SURF zijn er verschillende rollen (*mere conduit* als internetprovider; hostingdienst) die onder de DSA vallen. Zie aandachtspunt 3 voor een uiteenzetting hiervan.

Digital Markets Act (DMA)

Kern van de regeling

- De DMA legt regels op aan online platforms die poortwachters (*gatekeepers*) zijn, om concurrentie op de digitale interne markt te verbeteren. Een onderneming wordt aangewezen als *gatekeepers* indien die:
  - Een aanzienlijke impact heeft op de Europese interne markt;
    - Concreet: als een kernplatformdienst* in drie lidstaten wordt aangeboden en indien de onderneming een jaaromzet van € 7,5 miljard of marktkapitalisatie van € 75 miljard heeft.
  - Een kernplatformdienst aanbiedt die voor zakelijke gebruikers een belangrijke toegangspoort tot eindgebruikers vormt;
    - Concreet: minstens 45 miljoen maandelijks actieve eindgebruikers in de EU en 10.000 jaarlijks actieve zakelijke gebruikers in de EU.
  - Met betrekking tot haar activiteiten een stevig verankerde en duurzame positie inneemt of naar verwachting in de nabije toekomst een dergelijke positie zal innemen.
    - Concreet: de genoemde gebruikersaantallen moeten in elk van de laatste drie boekjaren gehaald zijn.

Verwachte impact

- Verwachte impact OCW: **KLEIN**
- Verwachte impact veld: **KLEIN**
  - Er zijn geen partijen in de beleidsterreinen van OCW die aan de criteria voor poortwachters voldoen. Alle impact is dus indirect.

DMA

De DMA is op 14 september 2022 getekend. Inwerkingtreding wordt daarmee verwacht in oktober of november 2022. Zes maanden later is de DMA rechtstreeks van toepassing.

Fase 1 OPSTELLEN VOORSTEL

Fase 2 VOORSTEL IN ONDERHANDELING

Fase 3 INWERKINGTREDING

* De volgende diensten zijn kernplatformdiensten:
a) onlinetussenhandelsdienst;
b) onlinezoekmachine;
c) online socialenetwerkdienst;
d) videoplatformdienst;
e) nummeronafhankelijke interpersoonlijke communicatiedienst;
f) besturingssysteem;
g) webbrowser;
h) virtuele assistent;
i) cloudcomputingdienst;
j) onlineadvertentiedienst, waaronder advertentienetwerken, advertentie-uitwisselingsdiensten en andere advertentietussenhandelsdiensten, aangeboden door een onderneming die een van de in de punten a) tot en met i) genoemde kernplatformdiensten aanbiedt;

dialogic innovatie • interactie

DMA – relatie tot andere regelgeving

- De DMA is een verordening en heeft dus directe werking.
- De DMA wordt vaak samen genoemd met de Digital Services Act (DSA), zij vormen samen het Digital Services Package. Waar de DMA over het bevorderen van eerlijke concurrentie in de digitale interne markt, gaat de DSA over het bestrijden van illegale inhoud.
- De DMA bevat enkele regels met betrekking tot het verwerken van persoonsgegevens door poortwachters en heeft daarmee een aanvullende werking op de GDPR. De DMA doet geen afbreuk aan de GDPR.

DMA – rechten en plichten

Doelgroep

- De poortwachters waarop deze wetgeving zich richt betreffen grote online platforms. Het gaat (in principe) om diensten met minstens 45 miljoen maandelijks actieve eindgebruikers en minstens 10.000 jaarlijks actieve zakelijke gebruikers, aangeboden door ondernemingen met een jaarlijkse omzet van € 7,5 miljard of een marktkapitalisatie van € 75 miljard.*
- Gelet op deze criteria is het onwaarschijnlijk dat partijen in de beleidsterreinen van OCW als poortwachter aangewezen zullen worden.

Inhoud

- De DMA bevat regels voor poortwachters die een eerlijker speelveld creëren voor zowel concurrenten van poortwachters als voor de zakelijke gebruikers van de diensten van poortwachters, evenals regels ten behoeve van eindgebruikers. Bijvoorbeeld:
  - Poortwachters mogen niet verhinderen dat een zakelijke gebruiker via diensten van derden dezelfde producten aan eindgebruikers aanbiedt voor een lagere prijs dan via de dienst van de poortwachter.
  - Poortwachters mogen persoonsgegevens die afkomstig zijn van hun kernplatformdienst niet (zonder toestemming) gebruiken in andere diensten die zij aanbieden.

* Onder omstandigheden kan de EC ook aanbieders die niet aan elk van deze eisen voldoen aanwijzen als poortwachter.

DMA - Relevantie voor de OCW-beleidsterreinen

Impact

- Wij zien geen directe impact voor in Nederland gevestigde bedrijven in OCW-sectoren.
- Indirecte impact zal voornamelijk bestaan uit het verwezenlijken van eerlijkere marktposities voor zakelijke gebruikers van diensten van gatekeepers. Ter illustratie: indien aanbieders van elektronische leeromgevingen (hypothetisch) oneerlijke concurrentie zouden ondervinden van Google Classroom, doordat Google zijn poortwachtersfunctie zou misbruiken, zou de DMA dit kunnen tegengaan.
- Vanwege een positief effect op concurrentie tussen diensten kunnen ook eindgebruikers van allerlei diensten (bijvoorbeeld scholen of culturele instellingen) een beter dienstenaanbod krijgen.
- Indirecte impact zou ook kunnen bestaan uit doorberekende kosten van gatekeepers aan hun zakelijke gebruikers of eindgebruikers.

AI

AI Act

Artificial Intelligence Act (AI Act)

Kern van de regeling

- De AI Act heeft als doel om te zorgen dat AI-systemen die in de EU op de markt worden gebracht en gebruikt, veilig zijn en in overeenstemming zijn met de geldende fundamentele rechten en waarden binnen de EU.
- Het voorstel onderscheidt drie categorieën AI-systemen en stelt regels op per categorie:
  - Verboden praktijken/systemen met onaanvaardbare risico's
  - Hoogrisicosystemen (waaronder veel systemen voor onderwijs)
  - Laagrisicosystemen
- Los van deze indeling bevat de regeling transparantieverplichtingen voor bepaalde typen systemen.

Verwachte impact

- Verwachte impact OCW: **KLEIN**
- Verwachte impact veld: **MEDIUM**
  - Wetenschappers kunnen in aanraking komen met de AI act in publiek-private samenwerkingen
  - Voor een aantal toepassingen in het onderwijs is sprake van hoogrisicosystemen, daar moet rekening mee worden gehouden bij inkoop en inzet. Dit betreft onder andere *adaptive learning*. Dit is het deel waar we de grootste impact voorzien.

AI Act

De Commissie heeft 21 april 2022 voorstel voor de AI Act gepresenteerd. Het is op moment van schrijven in onderhandeling.

Fase 1 OPSTELLEN VOORSTEL

Fase 2 VOORSTEL IN ONDERHANDELING

Fase 3 INWERKINGTREDING

dialogic innovatie • interactie

AI Act – relatie tot andere regelgeving

- De AI Act heeft directe werking.
- Europese wetgeving m.b.t. bescherming van persoonsgegevens (de AVG) blijft van kracht.
- De AI Act biedt onder bepaalde omstandigheden een wettelijke grondslag om bijzondere categorieën persoonsgegevens te verwerken, voor zover dit strikt noodzakelijk is om de monitoring, opsporing en correctie van vertekeningen te waarborgen in verband met AI-systemen met een hoog risico.
- Vanuit de verschillende regelgevingen op datagebied (ODD, DGA, DA) wordt beschikbaarheid van bestaande datasets voor verdere ontwikkeling van AI gestimuleerd. Het ontsluiten van kwalitatief goede datasets past bij de in de AI Act gestelde eisen aan AI-ontwikkeling.

AI Act – rechten en plichten

Definities en doelgroep

- De definitie van AI-systeem is erg breed en omvat bijvoorbeeld ook geautomatiseerde beslisregels. Zie onderstaande box voor de volledige definitie uit de meest recente compromistekst.
- Er worden zowel eisen gesteld aan de systemen zelf, als aan de aanbieders en gebruikers van de systemen. Er zijn drie opties voor wie de verantwoordelijke partij is:
  - De ontwikkelaar is verantwoordelijk als die het systeem zelf in de praktijk brengt, ook wanneer het verder niet op de markt komt.
  - De partij die het systeem op de markt brengt is verantwoordelijk in alle gevallen waar het systeem wordt ingezet conform de instructies, voor het doel waarvoor de partij het aanbiedt.
  - De partij die het systeem inzet is verantwoordelijk wanneer zij een AI-systeem inzet voor een doel dat anders is dan het beoogde doel van de aanbieder/ontwikkelaar.

Article 3 - Definitions
'artificial intelligence system' (AI system) means a system that is designed to operate with a certain level of autonomy and that, based on machine and/or human-provided data and inputs, infers how to achieve a given set of human-defined objectives using machine learning and/or logic- and knowledge based approaches, and produces system-generated outputs such as content (generative AI systems), predictions, recommendations or decisions, influencing the environments with which the AI system interacts;

AI Act – rechten en plichten

Systemen met onaanvaardbaar risico

- Kort gezegd zijn AI-systemen die mensen manipuleren of kwetsbaarheden exploiteren en die waarschijnlijk fysieke of psychologische schade tot gevolg hebben verboden. Ook social scoring door of namens overheden is in veel gevallen verboden, net als real-time biometrische identificatie met het oog op rechtshandhaving.

Transparantieverplichtingen voor bepaalde AI-systemen

- Aanbieders zorgen ervoor dat AI-systemen die voor interactie met natuurlijke personen zijn bedoeld, zodanig worden ontworpen en ontwikkeld dat natuurlijke personen worden geïnformeerd dat zij interageren met een AI-systeem, tenzij de omstandigheden en de gebruikscontext dit duidelijk maken.
- Gebruikers van een emotieherkenningssysteem of een biometrisch indelingssysteem informeren de daaraan blootgestelde natuurlijke personen over de werking van het systeem.
- Gebruikers van AI-systemen die deep fakes maken moeten bekend maken dat het materiaal kunstmatig is verwerkt of gegenereerd.

AI Act – rechten en plichten

Systemen met hoog risico*

Deze categorie is relevant voor OCW omdat bepaalde AI-systemen met betrekking tot onderwijs en beroepsopleiding hiertoe behoren. Voor deze systemen gelden globaal de volgende eisen:

- Er moet een systeem voor risicobeheer worden vastgesteld, uitgevoerd, gedocumenteerd en in stand gehouden. Dit moet een doorlopend iteratief proces zijn, tijdens de gehele levensduur van het AI-systeem. Het behelst het inschatten van risico's in verschillende situaties, het evalueren van die risico's en het vaststellen van risicobeheersingsmaatregelen. Hier worden verschillende eisen aan gesteld.
- Eventuele data die worden gebruikt voor het trainen, valideren en testen van modellen moet aan bepaalde kwaliteitseisen voldoen. Deze eisen zien zowel op passende praktijken op het gebied van databeheer als op de kwaliteit van de data zelf.**
- Er worden onder meer eisen gesteld aan technische documentatie, loggingscapaciteiten, transparantie en informatieverstrekking richting gebruikers, menselijk toezicht, nauwkeurigheid, robuustheid en cyberbeveiliging van de AI-systemen.
- Het AI-systeem moet geregistreerd worden in een EU-database, beheerd door de Europese Commissie. Ook de aanbieder wordt hierin geregistreerd. In de database dient ook het zogeheten *real world testing* geregistreerd te worden.

Aanbieders van AI-systemen met een hoog risico moeten zorgen dat het AI-systeem aan de eisen voldoet en blijft voldoen. Ook moeten zij voorzien in een systeem voor kwaliteitsbeheer, een conformiteitsprocedure uitvoeren en aan enkele andere verplichtingen voldoen.

Ook op **importeurs, distributeurs en gebruikers** rusten verplichtingen. Deze hebben met name betrekking op het controleren van de conformiteitsmarkering en van de aanwezigheid van de vereiste documentatie en gebruiksinstructies. Gebruikers dienen de gebruiksinstructies op te volgen, zij mogen het systeem dus alleen gebruiken voor de vastgestelde doeleinden.

Wanneer een **overheidsorganisatie** een hoogrisicosysteem wil gebruiken moet zij zich vooraf in de EU-database registreren en daarbij selecteren welke systemen zij wil gebruiken. Sommige organisaties, zoals rechtshandhaving, zijn hiervan uitgezonderd.

*Hoogrisicosystemen zijn in de meest recente tekst als volgt gedefinieerd:

Article 6 - Classification rules for high-risk AI systems

AI systems referred to in Annex III shall be considered high-risk in any of the following cases:

a) the output of the system is immediately effective with respect to the intended purpose of the system without the need for a human to validate it;

b) the output of the system consists of information that constitutes the sole basis or is not purely accessory in respect of the relevant action or decision to be taken by the human, and may therefore lead to a significant risk to the health, safety or fundamental rights.

De Commissie kan Bijlage 3 onder bepaalde voorwaarden aanpassen via delegated acts.

** De data moeten bijvoorbeeld relevant, representatief, foutenvrij en volledig zijn. Ook moeten zij de passende statistische kenmerken hebben.

AI Act – Relevantie voor de OCW-beleidsterreinen

Impact onderwijs

- Er zijn twee categorieën hoogrisicotoepassingen in het onderwijs. Mede op voorstel van Nederland, na consultatie door OCW van relevante partijen, zijn deze in de recente compromistekst aangescherpt. Met name sub b in onderstaande box verdient extra aandacht. In de vorige versie was deze (slechts) gericht op het beoordelen van studenten en het beoordelen van toelatingstoetsen. In deze versie bestrijkt het **leeruitkomsten** en **het leerproces**. Dit is een significant breder toepassingsgebied. Hiermee wordt in ieder geval *adaptive learning* als hoogrisicotoepassing gedefinieerd. Afhankelijk van interpretatie kunnen ook bepaalde toepassingen op het vlak van *learning analytics* hieronder worden geschaard.
  - Belangrijke beperking van de scope is dat de systemen die de AI Act noemt volgens de recente compromistekst alleen als hoogrisicosysteem worden aangemerkt in het geval van automatische besluitvorming zonder menselijke validatie, of indien het systeem de enige beslissende factor is of 'niet puur ondersteunend'* is en daardoor een significant risico voor gezondheid, veiligheid of fundamentele rechten vormt. Zolang sprake is van menselijke tussenkomst zal vermoedelijk dus nog redelijk veel mogelijk blijven zonder dat de eisen die aan hoogrisicotoepassingen worden gesteld van toepassing zijn. Veel zal echter afhangen van de uitleg van het begrip *purely accessory* en van de interpretatie omtrent 'significant risk to fundamental rights'.
- De eisen die aan hoogrisicosystemen worden gesteld maken het moeilijker om deze producten te ontwikkelen. Dit geldt met name voor nieuwe of kleine aanbieders, bijvoorbeeld omdat ze niet over voldoende representatieve trainingsdata beschikken om een model goed genoeg te trainen. In algemene zin is aannemelijk dat de AI Act een beperkend effect zal hebben op het aanbod en de innovatie van deze diensten, doordat (potentiële) leveranciers aan de eisen moeten voldoen. Zie aandachtspunt 4 voor de verwachte impact op onderwijsinnovatie.

Article 6 - Classification rules for high-risk AI systems
AI systems referred to in Annex III shall be considered high-risk in any of the following cases:
a) the output of the system is immediately effective with respect to the intended purpose of the system without the need for a human to validate it;
b) the output of the system consists of information that constitutes the sole basis or is not purely accessory in respect of the relevant action or decision to be taken by the human, and may therefore lead to a significant risk to the health, safety or fundamental rights.

ANNEX III - HIGH-RISK AI SYSTEMS REFERRED TO IN ARTICLE 6
3. Education and vocational training:
a) AI systems intended to be used for the purpose of determining access, admission or assigning natural persons to educational and vocational training institutions or programmes at all levels;
b) AI systems intended to be used for the purpose of assessing natural persons with the view of evaluating learning outcomes or steering the learning process in educational and vocational training institutions or programmes at all levels.

*In de compromistekst is opgenomen dat de Commissie binnen een jaar na inwerkingtreding nader zal specificeren wat *purely accessory* inhoud in het kader van de relevante categorieën in bijlage 3.

AI Act – Relevantie voor de OCW-beleidsterreinen

Impact onderzoek en wetenschap

- De ontwikkeling van AI-systemen voor zuiver wetenschappelijke doeleinden valt niet binnen de *scope* van de AI Act. Hetzelfde geldt voor de ontwikkeling van AI-systemen in R&D, zolang ze niet in de praktijk worden gebracht. Uiteraard kan het feit dat de eisen toepasselijk worden wanneer een systeem in de praktijk wordt gebracht, ook invloed hebben op R&D. Zelfs als nog onduidelijk is of een systeem ooit in praktijk zal worden gebracht, kan namelijk wel op voorhand rekening met de eisen worden gehouden.
- Als wetenschappers in een samenwerking met het bedrijfsleven AI-systemen met een hoog risico ontwikkelen die in de praktijk worden gebracht, zijn de regels wél van toepassing.
- Voor onderzoek en ontwikkelingen van hoogrisicotoepassingen liggen mogelijkheden voor *real-world testing* in zowel *regulatory sandboxes* als het aanvragen van ruimte om deze te testen buiten *sandboxes* om. Zie hiervoor ook aandachtspunt 4.

Impact cultuur

- Er zijn geen hoogrisicosystemen gedefinieerd die binnen de cultuursector vallen.
- Het is mogelijk dat in de cultuursector AI-systemen worden gebruikt die voor interactie met natuurlijke personen zijn bedoeld. Als gevolg van deze wet zal voor deze personen duidelijk moeten zijn dat zij interacteren met een AI-systeem.
- Een eerdere versie van het voorstel bevatte uitzonderingsmogelijkheden op de plicht om transparant te zijn over *deep fakes,* onder andere in het kader van het recht op vrijheid van kunsten. Deze uitzonderingen zijn geschrapt in de meest recente versie.

Data

ODD – DGA - DA

Open Data Directive (ODD)

Kern van de regeling

- De ODD is een herschikking van de PSI-richtlijn en gaat over hergebruik van overheidsinformatie.
- Het doel is om innovatie te stimuleren door het hergebruik van overheidsinformatie te stimuleren. Deze gegevens moeten de voortgang/ontwikkeling van met name kunstmatige intelligentie versterken, door grotere beschikbaarheid van trainingsdata. De ODD regelt dat bepaalde gegevens beschikbaar moeten worden gemaakt voor hergebruik en onder welke voorwaarden dat moet gebeuren.

Verwachte impact

- Verwachte impact OCW: **KLEIN**
- Verwachte impact veld: **KLEIN**

Open Data Directive

De ODD is juli 2019 in werking getreden. De implementatiewet ligt op moment van schrijven bij de Raad van State voor advies.

Fase 1 OPSTELLEN VOORSTEL

Fase 2 VOORSTEL IN ONDERHANDELING

Fase 3 INWERKINGTREDING

dialogic innovatie • interactie

ODD – relatie tot andere regelgeving

- De ODD is een herschikking van de *Directive on the re-use of public sector information* (PSI-richtlijn) uit 2003. Deze werd in 2013 al eens gewijzigd. de ODD (2019) is een update om het regelgevingskader aan te passen aan de vooruitgang op het gebied van digitale technologieën en om digitale innovatie verder te stimuleren.
- De ODD wordt geïmplementeerd door, via de Wet implementatie Open data richtlijn, de Wet hergebruik van overheidsinformatie (Who) en enkele andere wetten aan te passen.
- De ODD en de Who kunnen in tandem worden gezien met de Wet open overheid (Woo). De Woo regelt welke gegevens openbaar moeten zijn, de Who regelt hoe die openbare gegevens beschikbaar moeten worden gesteld voor hergebruik.
- Samen met de DGA en de DA heeft de ODD onder meer als doel om de beschikbaarheid van data voor het ontwikkelen van Artificiële Intelligentie (AI) vergroot. De ODD doet dit door regels op te stellen voor het zonder onderscheid beschikbaar stellen van bepaalde gegevens voor de samenleving.

ODD – rechten en plichten

Doelgroep

- In algemene zin richt ODD zich op overheidsorganisaties, overheidsondernemingen en publiekrechtelijke instellingen (zie kader). Hierop wordt een aantal uitzonderingen gemaakt. De uitzonderingen die relevant zijn voor het beleidsterrein van OCW lichten we in de volgende slide toe.
- ODD gaat specifiek over gegevens die worden gegenereerd bij het leveren van een dienst in het algemeen belang. Bedrijfsvoering van een publiekrechtelijke instelling is dat bijvoorbeeld doorgaans niet.
- Documenten met persoonsgegevens, bedrijfsgeheimen, statistische geheimen of intellectueel eigendom vallen **niet** onder de *scope* van ODD.

Rechten en plichten

- Onder ODD is het mogelijk om gegevens op te vragen bij bovenstaande typen organisaties. Op aanvraag moeten deze gegevens dan geleverd worden. Hierbij mag geen onderscheid worden gemaakt tussen aanvragers. Er mag wel een onkostenvergoeding aan verbonden zijn, die moet vooraf helder worden gecommuniceerd.
- Het na productie openbaar maken van gegevens wordt aangemoedigd, maar is niet vereist. Bij realtime-data wordt wel een API-toegang gevraagd.
- Van lidstaten wordt verwacht dat zij overzichtslijsten met beschikbare gegevens publiceren.

Publiekrechtelijke instellingen (art. 2 lid 2) zijn instellingen die voldoen aan de volgende kenmerken:

a) Zij zijn opgericht voor het specifieke doel te voorzien in andere behoeften van algemeen belang dan die van industriële of commerciële aard;
b) Zij bezitten rechtspersoonlijkheid; en
c) Zij worden merendeels door de staats-, regionale of lokale overheidsinstanties of andere publiekrechtelijke instellingen gefinancierd, of hun beheer staat onder toezicht van deze instanties of instellingen, of zij hebben een bestuurs-, leidinggevend of toezichthoudend orgaan waarvan de leden voor meer dan de helft door de staat, de regionale of lokale overheidsinstanties of andere publiekrechtelijke instellingen zijn aangewezen;

*Een kleine onderneming is een onderneming met minder dan 50 werknemers, waarvan de jaaromzet of het jaarlijkse balanstotaal 10 miljoen EUR niet overschrijdt. Als onderneming wordt beschouwd iedere eenheid, ongeacht haar rechtsvorm, die een economische activiteit uitoefent.

ODD – Relevantie voor OCW-beleidsterreinen

Impact onderwijs

- De ODD is niet van toepassing op documenten van onderwijsinstellingen voor primair of secundair onderwijs.
- Voor andere onderwijsinstelling geldt dat de ODD alleen van toepassing is op onderzoeksgegevens* en alleen voor zover deze gegevens publiek gefinancierd zijn en reeds openbaar zijn gemaakt.

Impact onderzoek en wetenschap

- Voor onderzoeksinstellingen en organisaties die onderzoek financieren is de ODD alleen van toepassing op onderzoeksgegevens en alleen voor zover deze gegevens publiek gefinancierd zijn en reeds openbaar zijn gemaakt.
- Lidstaten zijn vanuit de ODD verplicht beleid te ontwikkelen om Open Access en FAIR databeleid te stimuleren.

Impact cultuur

- Culturele instellingen zijn opgesplitst onder de ODD. Er zijn enkel verplichtingen voor **bibliotheken, archieven en musea.** Voor publieke omroepen en overige culturele instellingen zijn er uitzonderingen.
- Voor **archieven** is met de implementatiewet een wijziging voorgesteld in de Archiefwet, die aangewezen archiefbewaarplaatsen verplicht om te voldoen aan de Who.
- Bij digitalisering van cultureel erfgoed mag een verlengde periode van exclusiviteit worden toegekend aan de partij die de documenten digitaliseert.

- Onderzoeksgegevens zijn andere documenten in digitale vorm dan wetenschappelijke publicaties, die worden verzameld of geproduceerd tijdens wetenschappelijke onderzoeksactiviteiten en die als bewijs in het onderzoeks-proces worden gebruikt, of waarvan binnen de onderzoeksgemeenschap algemeen wordt erkend dat ze noodzakelijk zijn om onderzoeksresultaten te valideren.

Data Governance Act (DGA)

Kern van de regeling

- De DGA reguleert drie hoofdzaken:
  - Gegevens die vanwege hun inhoud buiten de scope van de ODD vallen (persoonsgegevens, handelsgeheimen, statistische geheimen en intellectueel eigendom);
  - Databemiddelingsdiensten (diensten die zelf geen data bezitten, maar de uitwisseling tussen organisaties mogelijk maken); en
  - Data-altruïsme (het beschikbaar stellen van de eigen persoonsgegevens voor doelen in het algemeen belang).
- In alle gevallen is het doel om innovatie (m.n. in machine learning) te stimuleren door meer gegevens beschikbaar te maken voor (her)gebruik.

Verwachte impact

- Verwachte impact OCW: **KLEIN**
- Verwachte impact veld: **KLEIN-MEDIUM**
  - Zowel data-altruïsme als databemiddelingsdiensten bieden kansen voor onderzoek. Dit kan de beschikbaarheid van data vergroten en zorgen op privacygebied wegnemen bij onderzoekers.

Data Governance Act (DGA)

De DGA is juni 2022 in werking getreden. Vijftien maanden later wordt de DGA rechtstreeks van toepassing.

Fase 1 — OPSTELLEN VOORSTEL

Fase 2 — VOORSTEL IN ONDERHANDELING

Fase 3 — INWERKINGTREDING

dialogic innovatie • interactie

DGA – relatie tot andere regelgeving

- Hoofstuk II van de DGA bouwt voort op de ODD en geldt specifiek daar waar de ODD niet geldt. Het regelt de beschikbaarheid van gegevens die vanwege hun inhoud buiten de scope van de ODD vallen (persoonsgegevens, handelsgeheimen, statistische geheimen en intellectueel eigendom). Hiermee sluit het aan bij de doelstelling (ODD, DGA, DA) om een betere toegang tot gegevens te bieden voor de ontwikkeling van AI.
- Met de DGA wordt op alle vlakken de regie van burgers op eigen gegevens versterkt om AVG-rechten te borgen.
- De DGA heeft directe werking.

DGA – rechten en plichten

Hergebruik van beschermde overheidsinformatie (hoofdstuk II)

- Globaal is het doel van hoofdstuk II van de DGA om bepaalde beschermde gegevens toch **beschikbaar** te maken voor hergebruik. Merk op dat dit niet betekent dat deze gegevens openbaar worden.
- Onder bepaalde voorwaarden mogen gegevens met persoonsgegevens, bedrijfsgeheimen, statistische geheimen of intellectueel eigendom wel beschikbaar worden gesteld. Hierin krijgen publiekrechtelijke instellingen de verplichting om waar mogelijk toestemming voor hergebruik te regelen. Mogelijk hieraan verbonden voorwaarden zijn bijvoorbeeld: vertrouwelijkheidseisen, beveiligde toegang of enkel toegang *on-premises*.*
- De overheid moet zorgen voor een centraal informatiepunt dat verzoeken om hergebruik van de genoemde gegevens verwerkt.

Databemiddelingsdiensten (hoofdstuk III)

- Databemiddelingsdiensten bezitten zelf geen gegevens, maar brengen commerciële relaties tot stand om gegevens te delen. Dit kan met technische, juridische of andere middelen. Hoofdstuk III van de DGA reguleert deze diensten.
- Databemiddelingsdiensten kunnen twee verbindingen leggen:
  - Tussen gegevenshouder en gegevensgebruiker
  - Tussen datasubject en gegevensgebruiker (voor commerciële doeleinden, i.t.t. data-altruïsme)
- Databemiddelingsdiensten moeten zich bij een aan te wijzen autoriteit aanmelden voor certificering en regulering.

Data-altruïsme (hoofdstuk IV)

- Data-altruïsmediensten verbinden datasubjecten met organisaties die data verwerken in het algemeen belang, om op een makkelijke en gestandaardiseerde wijze (persoons)gegevens te kunnen ontsluiten.
- Lidstaten wijzen een of meer autoriteiten aan die verantwoordelijk zijn voor het registreren van erkende data-altruïsmediensten.
- De DGA stelt regels om voor registratie in aanmerking te komen, zo moet een organisatie voor data-altruïsme juridisch onafhankelijk zijn van enige entiteit met een winstoogmerk.
- Lidstaten kunnen nationaal beleid vaststellen om data-altruïsme verder te faciliteren.

* Volledige voorwaarden voor hergebruik kunnen worden gevonden onder artikel 5.

DGA – Relevantie voor OCW-beleidsterreinen

Impact onderwijs

- Gegevens in het bezit van onderwijsinstellingen zijn volledig uitgezonderd van hoofdstuk II van de DGA. Databemiddelingsdiensten en data-altruïsme zijn niet specifiek relevant voor onderwijsinstellingen. De DGA heeft dus geen impact op onderwijsinstellingen.

Impact cultuur

- Publieke omroepen zijn volledig uitgezonderd van hoofdstuk II. Overige culturele instellingen zijn ook in het geheel uitgezonderd van hoofdstuk II. Databemiddelingsdiensten en data-altruïsme zijn niet specifiek relevant voor de cultuursector. De DGA heeft dus geen impact op de cultuursector.

Impact op onderzoek en wetenschap

- Zowel data-altruïsme als databemiddelingsdiensten bieden kansen voor onderzoek. Hiermee kunnen onderzoeksgegevens systematisch ter beschikking worden gesteld aan onderzoekers met toestemming voor verwerking in het kader van (wetenschappelijk) onderzoek, via erkende en gereguleerde organisaties. Dit kan de beschikbaarheid van data vergroten en zorgen op privacygebied wegnemen bij onderzoekers.
- Voor specifiek data-altruïsme is het behulpzaam als de onderzoekssector zichzelf hierin organiseert. Waar databemiddelingsorganisaties inkoop van data faciliteren moet voor data-altruïsme een non-profitorganisatie bestaan. Dit is effectiever en efficiënter als het sectorbreed wordt georganiseerd. Voor verdere uitweiding, zie aandachtspunt 5.

Data Act (DA)

Kern van de regeling

- De Data Act heeft als doelen om een eerlijke verdeling van de waarde uit data onder actoren in de data-economie te stimuleren en om de toegang tot data, en het gebruik daarvan, te bevorderen.
- De DA is vooral gericht op IoT-apparaten (*Internet of Things*). Momenteel hebben producenten van IoT-apparaten vaak exclusief de toegang tot veel data die met het gebruik van die apparaten gegenereerd worden. Met de Data Act krijgen de gebruikers de regie over deze data.
- De DA moet daarnaast het overstappen tussen dataverwerkingsdiensten gemakkelijker maken.
- Verder regelt de DA nog enkele andere zaken, zoals toegang tot private data voor overheidsorganisaties in gevallen van uitzonderlijke noodzaak, bescherming van MKB tegen oneerlijke handelspraktijken, waarborgen tegen onrechtmatige dataoverdracht en de ontwikkeling van interoperabiliteitsstandaarden voor hergebruik van data.

Verwachte impact

- Verwachte impact OCW: **KLEIN**
- Verwachte impact veld: **MIDDEL**
  - Overstappen tussen dataverwerkingsdiensten zal zowel makkelijker als goedkoper worden en *vendor lock-in* daarmee kleiner.
  - Met standaardisering van dataruimten zal het uitwisselen van gedigitaliseerd cultureel erfgoed en media internationaal makkelijker worden.

Data Act

De Data Act is 24 februari 2022 als voorstel aangenomen door de Commissie. Het is op moment van schrijven in onderhandeling.

Fase 1 OPSTELLEN VOORSTEL

Fase 2 VOORSTEL IN ONDERHANDELING

Fase 3 INWERKINGTREDING

DA – relatie tot andere regelgeving

- De DA is lex generalis.
- De Data Act voegt na de ODD en DGA een derde categorie data toe in termen van beschikbaarheid voor ontwikkeling van AI. Waar de ODD en DGA voornamelijk overheidsgegevens betreffen (m.u.v. databemiddeling en data-altruïsme), betreft de DA gegevens die bij Internet-of-Things-producenten (overdracht op verzoek van klant) en clouddiensten (toegang voor klant volgens uniforme standaarden) opgeslagen zijn.

DA – rechten en plichten

Regels m.b.t. Internet of Things

- Gebruikers van IoT-apparaten moeten hun gegevens op een redelijke manier kunnen inzien en verzoeken kunnen indienen voor het overdragen van hun gegevens naar derden.
- Fabrikanten moeten ervoor zorgen dat de data standaard gemakkelijk toegankelijk zijn en moeten transparant zijn over de beschikbare data en wijze van toegang.
- Wanneer redelijkerwijs verwacht kan worden dat een IoT-apparaat door meerdere mensen gebruikt wordt, moet de fabrikant redelijke inspanningen leveren om te zorgen voor individuele toegang voor iedere gebruiker.
- Deze verplichtingen zijn niet van toepassing op data die wordt gegeneerd door producten van kleine bedrijven.

Regels m.b.t. dataverwerkingsdiensten

- De DA stelt eisen aan de aanbieders van cloud-, edge- en andere dataverwerkingsdiensten om het overstappen tussen diensten makkelijker te maken.
- Deze diensten moeten zorgen dat de afnemer bij het overstappen naar een andere aanbieder functionele gelijkwaardigheid kan behouden. Faciliteren van de overstap moet tevens gratis zijn. Dataverwerkingsdiensten mogen dit weigeren op grond van technische onhaalbaarheid, maar dan ligt de bewijslast daarvoor bij de dataverwerkingsdienst.

Interoperabiliteit binnen dataruimten

- In 2020 heeft de Europese Commissie een Europese datastrategie geformuleerd, waarin een aantal te ontwikkelen dataruimten is geïntroduceerd. Binnen deze dataruimten zou data toegankelijk moeten zijn voor andere gebruikers om innovatie te stimuleren.
- De Data Act stelt hierbij specifiek dat binnen dataruimten aan de daarbinnen afgesproken normen moet worden voldaan m.b.t. bijvoorbeeld datastructuren en licenties.
- De Europese Commissie kan reguleringsinstanties vragen om voor nieuwe dataruimten nieuwe standaarden op te stellen.
- Op dit moment wordt gewerkt aan dataruimten voor cultureel erfgoed en voor media. Nederland is bij beide initiatieven betrokken. Hiermee wordt uitwisseling van gegevens tussen lidstaten ook verbeterd.

DA – Relevantie voor OCW-beleidsterreinen

Impact OCW-beleidsterreinen

- De Data Act is generieke regelgeving. Partijen in de OCW-sectoren zullen er baat bij hebben wanneer zij gebruik maken van IoT-apparaten en meer regie over de data willen, of wanneer zij willen overstappen van de ene dataverwerkingsdienst naar de andere.
- De overstapkosten tussen dataverwerkingsdiensten moeten in het geheel verdwijnen. Daarnaast moet de toegang tot gegevens bij dataverwerkingsdiensten gestandaardiseerd worden tussen diensten, ook voor de gebruiker. Zie aandachtspunt 6 voor een verdere uitwerking van de impact.

(Geen) IoT in onderwijs

- Omdat hier voorafgaand aan dit onderzoek vragen over zijn gesteld noemen wij hier specifiek nog het volgende. Producten die primair als doel hebben om data te verwerken (zoals tablets) en software vallen niet onder de regels met betrekking tot IoT-apparaten. Dat betekent dat deze regels uit de Data Act niet van toepassing zijn op de data die worden gegenereerd met softwarediensten die op dit moment in het onderwijs worden gebruikt voor bijvoorbeeld adaptief leren (rekentuin, snap-IT, etc.). Er lijken op dit moment nauwelijks IoT-toepassingen in gebruik in het onderwijs en die worden ook niet verwacht in de nabije toekomst.

Impact op SURF als dienstenleverancier

- SURF levert in het onderwijs dataverwerkingsdiensten. Hierbij is het volgende van belang:
  - Diensten die zijn ontwikkeld waarbij de inhoud relevant is voor de dienst, worden niet geclassificeerd als dataverwerkingsdienst. De regels met betrekking tot het faciliteren van overstappen zijn dan dus niet van toepassing. Diensten waarbij de inhoud irrelevant is voor de uitvoering van de dienst kwalificeren wel als dataverwerkingsdienst. Denk hierbij bijvoorbeeld aan bestandsopslag.
  - Wanneer het een combinatie betreft waarin ‘generieke’ diensten specifiek gericht op de Nederlandse onderwijs- of onderzoekssector worden ontwikkeld, en gericht op integratie met andere systemen in de sector, zoals bijvoorbeeld SURF Drive, kunnen we op basis van dit onderzoek niet zeggen hoe de regels uitwerken. Wij raden SURF aan hiernaar te kijken. Gelet op het doel van de bepalingen (het beschermen van afnemers tegen de macht van de dienstenleverancier) zal de impact in deze context naar verwachting laag zijn.
- Zie de definities bij aandachtspunt 6 voor een overzicht over de dataverwerkingsdiensten waar de DA betrekking op heeft.

Cybersecurity
CSA – NIS2 - CRA

Cyber Security Act (CSA)

Kern van de regeling

- De CSA* bestaat uit twee delen:
  - Een versterking van de rol van het EU Agentschap voor Netwerk –en Informatiebeveiliging (ENISA)
  - Het inrichten van een Europees kader voor cyberbeveiligingscertificering
- Het doel is om certificering van cyberbeveiliging op een Europees niveau te standaardiseren. Hiermee moeten standaarden die nu nationaal worden bepaald geharmoniseerd worden.
- Deze verordening heeft met name verplichtingen voor de overheid, minder voor het bedrijfsleven.

Verwachte impact

- Verwachte impact OCW: **KLEIN**
- Verwachte impact veld: **KLEIN**

* (EU) 2019/881

Cyber Security Act (CSA)

De CSA is juni 2019 in werking getreden en is reeds van toepassing.

Fase 1 OPSTELLEN VOORSTEL

Fase 2 VOORSTEL IN ONDERHANDELING

Fase 3 INWERKINGTREDING

CSA

Relatie tot andere regelgeving

- Met de CSA wordt verordening 526/2013, waarmee ENISA werd opgericht, ingetrokken.
- De CSA heeft directe werking. In de Uitvoeringswet cyberbeveiligingsverordening zijn regels ter uitvoering vastgelegd.
- De CSA introduceert een Europees cybercertificeringskader, maar stelt geen eisen aan producten zelf. De CRA zal dit wel doen.

Impact op OCW-sectoren

- De CSA is generieke regelgeving en heeft geen specifieke impact op de OCW-sectoren. Wel kunnen partijen in de sectoren er baat bij hebben dat cyberbeveiligingscertificaten meer gestandaardiseerd worden.

Cyber Resilience Act (CRA)

Kern van de regeling

- Met de Cyber Resilience Act wil de commissie gemeenschappelijke eisen om de cyberveiligheid van Europese digitale producten, diensten en processen te versterken.
- Door de CRA zouden hardware- en softwareproducten op de markt moeten worden gebracht met minder kwetsbaarheden. Ook moet de CRA verzekeren dat fabrikanten veiligheid gedurende de levenscyclus van het product serieus nemen.
- Daarnaast moet de CRA omstandigheden creëren waarin gebruikers rekening kunnen houden met de cyberveiligheid van producten, wanneer zij producten met digitale elementen selecteren of gebruiken.

Relatie tot andere regelgeving

- De CSA introduceert een Europees cybercertificeringskader, maar stelt geen eisen aan producten zelf. De CRA zal dit wel doen.

Impact OCW-beleidsterreinen

- De CRA is generieke regelgeving en heeft geen specifieke impact op de OCW-beleidsterreinen.

Cyber Resilience Act (CRA)

De CRA is 15 september 2022 als voorstel aangenomen door de Commissie. Het is op moment van schrijven in onderhandeling.

Fase 1 OPSTELLEN VOORSTEL

Fase 2 VOORSTEL IN ONDERHANDELING

Fase 3 INWERKINGTREDING

Richtlijn Netwerk –en Informatiebeveiliging (NIS2)

Kern van de regeling

- De NIS2 is een herziening van de eerdere Network and Information Security Directive (NIS; 2016/1148). Met de herziening wordt de richtlijn aangepast aan bestaande behoeften en toekomstbestendig gemaakt.
- Een van de pijlers van de huidige NIS is dat essentiële sectoren/entiteiten worden gedefinieerd en worden verplicht om bepaalde veiligheidsmaatregelen te treffen. Met NIS2 worden hier sectoren aan toegevoegd en wijzigt dit in een lijst van essentiële entiteiten en een lijst van belangrijke entiteiten. Ook hogeronderwijsinstellingen en onderzoeksinstellingen komen (mogelijk) onder belangrijke entiteiten te vallen.

Verwachte impact

- Hogeronderwijsinstellingen en onderzoeksinstellingen zullen aan bepaalde regels op het gebied van cybersecurity moeten voldoen omdat zij worden aangemerkt als (mogelijke) belangrijke entiteiten. Momenteel loopt er een ander onderzoek, in opdracht van OCW, naar de impact van de NIS2 voor OCW.

NIS2

De NIS2 is 16 december 2020 als voorstel aangenomen door de Commissie. 10 november 2022 vindt de plenaire stemming plaats.

Fase 1 OPSTELLEN VOORSTEL

Fase 2 VOORSTEL IN ONDERHANDELING

Fase 3 INWERKINGTREDING

dialogic innovatie • interactie

NIS2 – relatie tot andere regelgeving

- Met de NIS2 wordt de NIS (2016/1148) ingetrokken.
- De huidige NIS is geïmplementeerd via de Wet beveiliging netwerk- en informatiesystemen (Wbni) en onderliggend besluit. Hierin zijn essentiële diensten aangewezen en de betreffende maatregelen vastgelegd. Vermoedelijk zal de NIS2 primair via aanpassing van de Wbni worden geïmplementeerd.
- De NIS2 is onderdeel van een breder pakket van bestaande instrumenten en voorstellen met betrekking tot de veerkracht van openbare en particuliere entiteiten. In het voorstel van NIS2 worden er een aantal aangehaald.
  - Een ander wetsvoorstel, namelijk de voorgestelde Critical Entities Resilience Directive (CER), spreekt van kritieke entiteiten. Deze groep overlapt met de essentiële entiteiten uit de NIS2. Waar de NIS(2) gaat over het beschermen tegen cyberaanvallen, gaat de CER over het kunnen weerstaan van andere dreigingen, zoals bijvoorbeeld aanslagen en natuurrampen.
  - De NIS2 vervangt sectorale bepalingen met betrekking tot cybersecurity die momenteel zijn opgenomen in de richtlijn 2019/1972, betreffende de vaststelling van het Europees wetboek voor elektronische communicatie.
  - Een voorstel voor een verordening betreffende digitale operationele veerkracht voor de financiële sector (COM(2020) 595 final), zal als lex specialis van de NIS2 worden beschouwd zodra beide wetteksten in werking zijn getreden.

NIS2 – rechten en plichten

Doelgroep

- De maatregelen in de NIS2 zijn vooral gericht op overheden. Daarnaast moeten essentiële en belangrijke entiteiten aan bepaalde eisen voldoen.

Regels m.b.t. lidstaten

- Lidstaten moeten zorgen voor nationale kaders voor cyberbeveiliging. Dit omvat onder meer het vaststellen van een nationale strategie voor cyberbeveiliging en het coördineren van de bekendmaking van kwetsbaarheden. Ook moeten lidstaten nationale autoriteiten aanwezen voor zaken als crisisbeheersing en toezicht.
- NIS2 stelt regels voor samenwerking tussen lidstaten op het gebied van cyberbeveiliging.
- Lidstaten moeten de uitwisseling van cyberbeveiligingsinformatie tussen entiteiten reguleren.
- Lidstaten moeten zorgen dat essentiële en belangrijke entiteiten aan bepaalde verplichtingen voldoen, zie hieronder.

Regels m.b.t. essentiële en belangrijke entiteiten

- NIS2 bevat een lijst essentiële entiteiten en een lijst belangrijke entiteiten. Voor essentiële entiteiten geldt een strikter regime.
- Er moeten passende en evenredige technische en organisatorische maatregelen worden genomen om cyberbeveiligingsrisico’s te beheren.
- Bij (significante) cyberbeveiligingsincidenten moeten de autoriteiten in kennis worden gesteld.

NIS2 – Relevantie voor OCW-beleidsterreinen

De impact van NIS2 voor OCW is onderwerp van een ander onderzoek dat momenteel voor OCW wordt uitgevoerd en dat meer de diepte in gaat dan dit onderzoek. Wij wijzen wel vast op de volgende punten:

Cyberbeveiligingsstrategie

- Relevant voor OCW is dat de cyberbeveiligingsstrategie, die lidstaten moeten opstellen, onder meer de volgende twee elementen moet bevatten:
  - Een beleid om cyberveiligheidsvaardigheden –en bewustzijn te vergroten
  - Een beleid om academische en onderzoeksinstituten te ondersteunen om cyberveiligheidstools en een veilige netwerkinfrastructuur te krijgen

Belangrijke entiteiten

- Met de komst van NIS2 worden "onderzoeksinstituten op het terrein van toegepast onderzoek en experimentele ontwikkeling met het oog op commerciële exploitatie van onderzoeksresultaten" aangemerkt als belangrijke entiteiten.
- Lidstaten mogen zelf bepalen of zij de Richtlijn ook van toepassing willen laten zijn op onderwijsinstellingen die kritische onderzoeksactiviteiten verrichten.

Digitale toekomst

EDI – Digital Decennium

Verordening Raamwerk Europese Digitale Identiteit (EDI)

Kern van de regeling

- De verordening EDI dient ter verbetering van eIDAS*. Het doel is om te zorgen voor veiligere en wederzijds erkende digitale identificatiemiddelen. Lidstaten moeten zelf voor deze oplossingen zorgen.
- Nieuw onderdeel van deze digitale identificatiemiddelen is de zogeheten **portemonnee** (wallet), waarin attributen bewaard kunnen worden en geverifieerd kunnen worden bij de uitgevende instantie. De genoemde voorbeelden zijn medische attesten en **diploma's**.
- In 2030 wil de EC op deze manier voor 80% van de EU-burgers een digitale ID beschikbaar hebben.

Verwachte impact

- Verwachte impact OCW: **KLEIN-MEDIUM**
  - Er liggen taken bij OCW en uitvoeringsorganisaties om zowel ontsluiten van gegevens (bijvoorbeeld diplomagegevens) als het ontvangen van gegevens (denk aan bijvoorbeeld Studielink) mogelijk te maken.
- Verwachte impact veld: **KLEIN-MEDIUM**
  - Dit zou tot een versimpelde studentadministratie moeten leiden in het hoger onderwijs, specifiek met Europese uitwisselingen

* 'Electronic Identities And Trust Services', 910/2014.

Verordenig EDI

De verordening EDI is 3 juni 2021 als voorstel aangenomen door de Commissie. Het is op moment van schrijven in onderhandeling.

Fase 1 OPSTELLEN VOORSTEL

Fase 2 VOORSTEL IN ONDERHANDELING

Fase 3 INWERKINGTREDING

EDI – relatie tot andere regelgeving

In EDI komen veel bestaande initiatieven en oplossingen bij elkaar. De belangrijkste interacties bespreken we hier.

Single Digital Gateway/Once-Only Technical System (OOTS)

- Via de Single Digital Gateway kunnen overheden en overheidsinstanties gegevens over burgers uitwisselen. Het idee is dat burgers met een eenmalige aanmelding online gegevens laten delen tussen verschillende instanties.
- Toegang tot de Single Digital Gateway moet met de eIDAS (toekomstig eID) digitale identificatiemiddelen mogelijk zijn.
- De portemonnee vanuit EDI komt **naast OOTS** te bestaan. OOTS is voor uitwisseling tussen overheden en instanties, de portemonnee moet gegevens –en documentenuitwisseling tussen verschillende actoren toestaan, dus niet enkel government-to-government.

Europese initiatieven omtrent studentengegevens

- Er bestaan verschillende initiatieven rondom studentengegevens, zoals het European Student Card initiative (ESCi), European Student Identifier (ESI) en Erasmus+.
- Het ESCi moet gebruik maken van ESI en uiteindelijk gelinkt worden aan de Single Digital Gateway.

Cybersecurity en privacy

- EDI is in lijn met de AVG omdat het de burger regie geeft over het delen van persoonsgegevens met organisaties en het ook mogelijk moet maken die toestemming in te trekken.
- EDI-oplossingen moeten voldoen aan de Europese cyberveiligheidscriteria. Volgens revisie 3 kunnen anders te middelen worden ingetrokken.

EDI – rechten en plichten

Diensten

- Onder de EDI moeten via één aanmelding de volgende dingen mogelijk zijn:
  - Identificatie (denk aan aanvragen van officiële documenten, maar bijvoorbeeld ook aan leeftijdsverificatie op YouTube om content af te schermen voor minderjarigen)
  - Uitwisseling van persoonsgegevens
  - Online ondertekenen van documenten
  - Register- en elektronische archiefdiensten
- Burgers moeten deze diensten overal in de Europese Unie kunnen gebruiken. De meerwaarde ten opzichte van de Single Digital Gateway/OOTS is dat gegevens ook gedeeld moeten kunnen worden met andere partijen dan overheidsorganisaties.
- Deze diensten worden geleverd door **gekwalificeerde vertrouwensdiensten**.

Portemonnee

- In de portemonnee moet **minimaal** een aantal attributen worden toegevoegd. Hier gaat het specifiek om overheidsgegevens die geverifieerd moeten kunnen worden bij de bron. De minimale attributen staan in bijlage VI (revisie 3) en het kader rechts.
- Waar mogelijk moeten de gekwalificeerde vertrouwensdiensten de echtheid kunnen verifiëren bij de uitgevende instantie.
- Er is nog geen duidelijkheid over de vorm waarin deze gegevens moeten worden uitgegeven en volgens welke standaarden deze moeten worden opgesteld. Tussen landen kunnen deze verschillend gedefinieerd zijn.
- Lidstaten moeten nog overeenkomen hoe het businessmodel (inzetbaarheid en kosten) van de portemonnee voor bedrijven eruit moet komen te zien. Daarbij moet specifiek rekening worden gehouden met inzet door het MKB.

Minimaal aan de *wallet* toe te voegen attributen

- Adres
- Leeftijd
- Geslacht
- Burgerlijke staat
- Familiesamenstelling
- Nationaliteit of burgerschap
- In onderwijs behaalde kwalificaties, titels en licenties
- Professionele kwalificaties, titels en licenties
- Publieke vergunningen en licenties
- Financiële –en bedrijfsgegevens

Lidstaten mogen dit zelf uitbreiden. Bovenstaande gegevens zijn in de regelgeving vastgelegd.

EDI – rechten en plichten

Relevantie voor OCW-gebieden

- EDI is hoofdzakelijk relevant voor het (hoger) onderwijs. Het is van belang dat de sector zich hierop aansluit om uitwisseling van gegevens, bijvoorbeeld bij inschrijving, mogelijk te maken.*
- OCW heeft aangegeven dat de wijze waarop de portemonnee voor minderjarigen wordt ingericht een aandachtspunt is. Hoewel de Commissie de portemonnee voor minderjarigen wil inzetten voor leeftijdsverificatie online, in het kader van *Better Internet for Kids* (BIK+), hebben de onderzoekers hier echter geen informatie over gevonden.

Totstandkomings– en implementatieproces

- Het proces verdient hier extra aandacht omdat er ruimte is voor beïnvloeding op een aantal momenten.
- Na inwerkingtreding brengt de Commissie binnen zes maanden een uitvoeringshandeling uit betreffende de portemonnee, waarin de minimale specificaties van de portemonnee worden gepubliceerd.
- Binnen twaalf maanden na inwerkingtreding moeten lidstaten voorstellen introduceren voor hun digitale identificatiemiddelen. Dit is inclusief portemonnee. Binnen achttien maanden moeten ze in werking zijn.
- In de overwegingen voorafgaand aan revisie 3 wordt aangegeven dat er ruimte is om verder te onderhandelen over de inwerkingtredingstermijnen.
- Specifiek relevant voor de sector is de totstandkoming van de standaarden voor de attributen in de portemonnee. Gegeven de termijnen is het van belang om hier op een vroeg stadium een begin mee te maken.

* Nederland is betrokken bij de Diploma Use Case binnen de European Blockchain Services Infrastructure. Daarmee bestaat er al relevante kennis binnen in ieder geval DUO.

Parallel wordt er ook al gewerkt aan de opzet van een *large scale pilot* in *digital credentials* vanuit RvIG en BZK. Dergelijke *large scale pilots* hebben een belangrijke plek in de uitrol van EDI.

Beleidsagenda Digitaal Decennium (Digital Decade)

Kern van het besluit

- De beleidsagenda voor het Digitaal Decennium (2020-2030) wordt als gezamenlijk besluit tussen de Europese Raad en het Europese Parlement gepubliceerd.
- In brede lijnen zet de agenda de visie voor digitale transformatie van economie en samenleving in het decennium tot 2030 uiteen en voor hoe om te gaan met de gevolgen. Het voor OCW meest relevante onderdeel hierin is het beleidsdoel om meer ICT'ers op te leiden.
- Met dit besluit wordt een monitoringsstructuur opgezet
  - Er is een aantal KPI's geformuleerd, waaronder het aantal ICT'ers. De overige hebben geen betrekking op OCW.
  - Lidstaten moeten een nationale strategische *roadmap* opstellen en die elke twee jaar updaten en rapporteren aan de Europese Commissie.
- Aanvullend op de mededeling Digitaal Kompas van maart 2021 (*Digital Decade*) en dit uitvoeringsbesluit (*Path to the Digital Decade*, september 2021) heeft de Commissie ook een Verklaring over digitale rechten en beginselen voorgesteld. Deze dient als basis voor beleidsmakers bij de omgang met of de ontwikkeling van nieuwe technologieën en de samenwerking tussen lidstaten, overheidsinstanties en andere partijen, aan een mensgerichte digitale transformatie. Over de tekst vinden momenteel nog onderhandelingen plaats. Na afronding zal deze door de Commissie, Raad en Parlement gezamenlijk ondertekend worden.
- Voor OCW zijn o.a. onderdelen relevant die gaan over publieke waarden, connectiviteit, digitale vaardigheden en toegang tot digitaal onderwijs, gendergelijkheid, AI en marktwerking.

Verwachte impact

- Verwachte impact OCW: **KLEIN**
- Verwachte impact veld: **KLEIN**

Digital Decade

Het voorstel voor het besuit *Path to the Digital Decade* is 15 september 2021 aangenomen door de Commissie en is nu in onderhandeling.

Fase 1 OPSTELLEN VOORSTEL

Fase 2 VOORSTEL IN ONDERHANDELING

Fase 3 INWERKINGTREDING

Aandachtspunten

Aandachtspunten

Aandachtspunten

Naast uitwerking van de 11 stukken wet –en regelgeving zijn in dit onderzoek ook zes specifieke aandachtspunten voor de beleidsterreinen van OCW geformuleerd. Deze zijn in de volgende slides uitgewerkt.

Aandachtspunt 1: Onzekerheid in de *scope* van tussenhandelsdiensten onder de DSA.

Er is een mate van onzekerheid in de vraag wat als tussenhandelsdienst wordt gekwalificeerd in de DSA, omdat de DSA is geschreven met het oog op economische activiteiten. Dit is echter niet opgenomen in de definities van tussenhandelsdiensten, waarmee de positie van bijvoorbeeld onderwijsinstellingen onduidelijk blijft.

Aandachtspunt 2: Contentmoderatieverantwoordelijkheden onder de DSA in OCW-beleidsterreinen.

Waar onderdelen van de dienstverlening van organisaties in het OCW-beleidsterrein kwalificeren als online platform moeten zij op deze platforms procedures instellen voor verwijdering van illegale content.

Aandachtspunt 3: SURF als *mere conduit*– of hostingdienst

SURF heeft meerdere verschillende rollen onder de DSA, afhankelijk van de dienst die zij levert. Voor zover de diensten niet gedekt worden door aandachtspunt 2 bespreken we ze onder aandachtspunt 3.

Aandachtspunt 4: Hoogrisicosystemen en innovatie in het onderwijs onder de AI-act

Veel AI-toepassingen met betrekking op onderwijs vallen onder de hoogrisicodefinities. Onder aandachtspunt 4 bespreken we waar daar sprake van is en wat de consequenties zijn voor innovatie.

Aandachtspunt 5: Coördineren van data-altruïsme

Met data-altruïsme kunnen onderzoeksgegevens systematisch ter beschikking worden gesteld aan onderzoekers. Onder aandachtspunt 5 bespreken we eventuele nationale coördinatie op dit vlak.

Aandachtspunt 6: Gevolgen van interoperabiliteitseisen aan dataverwerkingsdiensten

In de sector bestaat een angst voor *vendor lock-in* bij grote clouddiensten. De Data Act treft een aantal maatregelen om deze *lock-in* terug te dringen. De verwachte impact bespreken we onder aandachtspunt 6.

1. DSA: Onzekerheid toepasselijkheid op onderwijs en onderzoek

Juridische interpretatie tussenhandelsdienst

- Wij kunnen op basis van dit onderzoek niet met zekerheid zeggen of diensten in het kader van onderwijs en onderzoek juridisch ook als tussenhandelsdienst kunnen kwalificeren. Uit verschillende bepalingen blijkt namelijk dat de verordening is geschreven met economische activiteiten in het hoofd, zie bijvoorbeeld overweging (5) hieronder. In de versie van 5 juli 2022 zijn tussenhandelsdiensten ook expliciet gedefinieerd als een subset van 'diensten van de informatiemaatschappij', wat in het oorspronkelijke voorstel niet zo was.
  - **Overweging (5)**: "Deze verordening moet van toepassing zijn op aanbieders van bepaalde diensten van de informatiemaatschappij zoals gedefinieerd in Richtlijn (EU) 2015/1535 van het Europees Parlement en de Raad, dat wil zeggen elke dienst die **gewoonlijk tegen vergoeding**, langs elektronische weg, op afstand en op individueel verzoek van een afnemer wordt verricht." (nadruk door onderzoekers)
- In een onafhankelijk onderzoek in opdracht van de Europese Commissie werd ook geconstateerd dat er enige onduidelijkheid is en werd aanbevolen dit aan te passen:
  - "The study shows that the pDSA may have an impact on research institutions, repositories and researchers. The pDSA is drafted with economic services in mind. This should be more clearly reflected in the DSA and could mitigate the implications of the pDSA to research institutions, repositories and researchers. Generally, organisations providing services that cannot be considered as economic services should be excluded from the ambit of the DSA."*

Juridische definities (art. 2(f) en 2(h) DSA)

"tussenhandelsdienst": een van de volgende diensten:

- *een "mere conduit"-dienst die bestaat in het doorgeven in een communicatienetwerk van door een afnemer van de dienst verstrekte informatie, of in het verstrekken van toegang tot een communicatienetwerk;*
- *een "caching"-dienst die bestaat in het doorgeven in een communicatienetwerk van door een afnemer van de dienst verstrekte informatie, waarbij die informatie automatisch, tussentijds en tijdelijk wordt opgeslagen met als enige doel om de latere doorgifte van die informatie aan andere afnemers van de dienst op hun verzoek doeltreffender te maken;*
- *een "hosting"-dienst die bestaat in de opslag van de door een afnemer van de dienst verstrekte informatie, op diens verzoek;*

"onlineplatform": een aanbieder van een hostingdienst die, op verzoek van een afnemer van de dienst, informatie opslaat en verspreidt bij het publiek, tenzij […]

Gewijzigde definitie van tussenhandelsdienst in meest recente tekst (art. 2(f) DSA)

*'intermediary service' means one of the following **information society** services: […]*

* Lundqvist (2022), Study on the Digital Services Act and Digital Markets Act and their possible impact on research.

2. DSA: Contentmoderatie in OCW-beleidsterreinen

Verantwoordelijkheden voor online platforms

- Onder de DSA moeten online platforms die inhoud beschikbaar maken voor anderen zorgen dat illegale content (zie rechts) wordt verwijderd als zij er kennis van hebben.
- Om illegale content te modereren moeten platforms een aantal dingen organiseren:
  - Ze moeten een klachtenprocedure hebben, waarbij naar de klager feedback wordt gegeven over besluiten omtrent hun klacht.
  - Bij verwijdering moeten ze aan de uploader aangeven waarom het materiaal verwijderd is.
  - Als een *trusted flagger* (zie rechts) aangeeft dat ze illegaal materiaal hebben aangetroffen moet de klacht met prioriteit en zonder vertraging verwerkt worden.
- Dit betekent **niet** dat een online platform zelf elk stukje illegale content moet vinden, maar bovenal dat er een goede procedure moet zijn om illegale content te verwijderen.
- In principe is de **leverancier** van het platform verantwoordelijk hiervoor, maar het kan wenselijk zijn om de regie hier wel zelf over te voeren. Ook zou de leverancier dit kunnen afdwingen. De exacte verdeling van verantwoordelijkheden kan contractueel bepaald worden.

Online platforms in onderwijs en onderzoek (zie kader rechts voor uitzonderingen)

- Onderwijs
  - Webfora (bijvoorbeeld onderdeel van ELO), ouderportalen en alle gelegenheden waar *comments* kunnen worden geplaatst.
  - Elektronische leeromgevingen. Het gaat dan niet alleen om fora, maar ook om bij vakken of modules geüploade materialen. Scans van bepaalde boeken of artikelen kunnen bijvoorbeeld verboden zijn om te delen.
- Onderzoek
  - *Repositories* voor gegevens en publicaties.
- Cultuur
  - Platforms waarop gebruikers commentaren kunnen plaatsen of bijvoorbeeld afbeeldingen delen kunnen hieronder vallen.

Illegale content

Bij illegale content gaat het om materiaal dat niet mag volgens de wet of de rechtmatige eigenaar van het materiaal. Dat kan dus gaan om bedreigingen, smadelijke uitspraken of kinderporno. Anderzijds kan het ook gaan over teksten waarop *copyright* rust, bijvoorbeeld (scans van) schoolboeken.

Trusted flagger

Een *trusted flagger* is een door de overheid erkende organisatie die gespecialiseerd is in het opsporen van illegaal materiaal online.

Uitzonderingen

De DSA bevat een uitzondering voor micro -en kleine ondernemingen onder de Europese definities van KMO's (Aanbeveling 2003/361/EG). Deze definities betreffen personeel (max 50 fte) en omzet/balanstotaal (beide max €10mln).

3. DSA: SURF en instellingen als *mere conduit*– of hostingdienst

De rol van SURF en anderen als internetprovider

- SURF fungeert als internetprovider voor Nederlandse onderwijsorganisaties. Onder de DSA kwalificeert het leveren van internet in principe als *mere conduit*-dienst. Ook hier geldt echter de onzekerheid van aandachtspunt 1: is dit een dienst van de informatiemaatschappij?
- In deze rol is de leverancier van de *mere conduit* dienst niet aansprakelijk voor doorgegeven informatie als:
  - Hij zelf niet het initiatief heeft genomen voor doorgifte
  - De ontvanger van de gegevens niet door hem wordt uitgekozen
  - De doorgegeven gegevens niet door hem worden geselecteerd of gewijzigd.
- Daarbovenop moet SURF in het kader van deze dienst, indien deze inderdaad een *mere* conduit-dienst is, in deze context aan de regels voldoen die voor alle tussenhandelsdiensten gelden. Zie daarvoor ook de bespreking van de DSA.
- Een vergelijkbaar aandachtspunt geldt voor andere situaties. Wanneer een instelling bijvoorbeeld kantoorruimte aan een bedrijf verhuurt wordt daarbij ook internet doorgegeven. Binnen de scope van dit onderzoek kunnen wij niet zeggen wanneer dit onder de DSA zou beschouwd zou worden als *mere conduit*-dienst. Wanneer dit zo is, zouden de basisverplichtingen voor tussenhandelsdiensten van toepassing zijn. De instelling zou dan onder meer een vast contactpunt voor autoriteiten moeten inrichten en, tenzij het een kleine onderneming is, jaarlijks moeten rapporteren over de verrichte inhoudsmoderatie. Wij merken hierbij op dat inhoudsmoderatie in principe enkel zou kunnen bestaan uit het niet langer leveren van de dienst aan de betreffende afnemer, aangezien er geen informatie op wordt geslagen en er dus geen sprake kan zijn van het verwijderen van illegale inhoud.

De rol van SURF als hostingdienst

- SURF regelt de opslag van veel gegevens voor onderwijs –en onderzoeksinstellingen. Denk hierbij bijvoorbeeld aan de SURF drive.
- De leverancier van een hostingdienst is niet aansprakelijk voor opgeslagen informatie als:
  - Hij geen kennis heeft van illegale content
  - Hij handelt om illegale content te verwijderen of af te sluiten zodra hij er kennis van heeft.
- Daarbovenop moet SURF in deze context aan de regels voldoen die voor alle tussenhandelsdiensten gelden. Zie daarvoor ook de bespreking van de DSA.

Mere conduit

Een *mere conduit* dienst faciliteert het doorgeven van informatie in een communicatienetwerk, dus bijvoorbeeld toegang tot het internet.

Hostingdiensten

Een hostingdienst voorziet in opslag van gegevens.

4. AI Act: Hoogrisicosystemen in het onderwijs

Hoogrisicosystemen in het onderwijs

- De definities uit de tweede compromistekst (juli 2022) dekken elke toepassing van AI die invloed heeft op het leerproces of de leeruitkomsten van een student, met uitzondering van systemen met menselijke tussenkomst die puur ondersteunend zijn en/of geen significant risico vormen voor gezondheid, veiligheid of fundamentele rechten. Zie de definities hieronder en de slides over de AI Act.
- De belangrijkste groep die onder deze nieuwe afbakening valt is **adaptief leren**. Veel toepassingen voor adaptief leren zullen met de huidige definities worden geclassificeerd als hoogrisicosysteem, omdat sprake is van een automatisch beslissingsproces dat invloed heeft op het leerproces.
- Bij andere toepassingen van AI in het onderwijs, zoals modellen om studie-uitkomsten te voorspellen of het leerpad te sturen, is over het algemeen sprake van menselijke tussenkomst. In dat geval is de classificatie afhankelijk van of er sprake is van een significant risico en van de aangekondigde toekomstige duiding van de Commissie van het begrip *purely accessory*.

CE-markering en conformiteitsverklaring

- De aanbieder dient een hoogrisicosysteem voor onderwijs zelf te voorzien van een CE-markering en dient zelf een EU-conformiteitsverklaring op te stellen en te tekenen. Hiermee neemt de aanbieder verantwoordelijkheid voor de conformiteit van het systeem aan de eisen die de AI Act stelt. Bij systemen voor onderwijs is sprake van een 'interne controle': de aanbieder verklaart zelf aan de eisen te voldoen, zonder controle door een overheidsinstelling.

Article 6 - Classification rules for high-risk AI systems
AI systems referred to in Annex III shall be considered high-risk in any of the following cases:
a) the output of the system is immediately effective with respect to the intended purpose of the system without the need for a human to validate it;
b) the output of the system consists of information that constitutes the sole basis or is not purely accessory in respect of the relevant action or decision to be taken by the human, and may therefore lead to a significant risk to the health, safety or fundamental rights.

ANNEX III - HIGH-RISK AI SYSTEMS REFERRED TO IN ARTICLE 6
3. Education and vocational training:
a) AI systems intended to be used for the purpose of determining access, admission or assigning natural persons to educational and vocational training institutions or programmes at all levels;
b) AI systems intended to be used for the purpose of assessing natural persons with the view of evaluating learning outcomes or steering the learning process in educational and vocational training institutions or programmes at all levels.

Hoogrisicosystemen

Hoogrisicosystemen zijn AI-systemen die in een vakgebied of sector vallen die door de Commissie wordt gedefinieerd als hoogrisico. Hoogrisicosystemen **moeten** een CE-markering hebben voordat ze op de markt mogen komen of mogen worden ingezet.

De Commissie kan deze categorieën uitbreiden. De eerste categorieën staan beschreven in bijlage III (zie kader voor onderwijs).

CE-markering

De CE-markering geeft aan dat een product voldoet aan de relevante Europese regulering. In het geval van AI-toepassingen betekent dat dus de AI Act. De exacte eisen staan in hoofdstuk 2 van de AI Act. Ze omvatten in ieder geval:

- Een goed risicomanagementsysteem
- Kwalitatief goede trainingsdata die verantwoord is verkregen en verwerkt
- Goede modelkeuzes
- Goede technische documentatie
- Transparantie naar gebruikers

4. AI Act: Hoogrisicosystemen in het onderwijs 2/2

Impact op innovatie

- Het aanwijzen van toepassingen als hoogrisicosystemen verbindt eisen aan het product en maakt het daardoor moeilijker voor nieuwe partijen om producten te ontwikkelen, bijvoorbeeld omdat ze niet over voldoende representatieve trainingsdata beschikken om een model goed genoeg te trainen.
- Partijen die reeds gevestigd zijn in een markt hebben vaak ook toegang tot meer gegevens en kunnen zodoende makkelijker een systeem ontwikkelen dat aan de eisen voldoet.
- Om de mogelijkheden voor innovatie te verbreden biedt de AI Act twee mogelijkheden:
  - *Regulatory sandboxes*, door de competente autoriteit aangewezen ruimtes waarin projecten kunnen worden ontwikkeld voor een specifieke toepassing.
  - *Real-world testing plans*, waarin een ontwikkelaar een plan moet indienen om binnen bepaalde kaders een toepassing te mogen testen. Dit geldt ook voor hoogrisicosystemen. Hierbij is toestemming van de testlocatie nodig.

Specificaties van regulatory sandboxes

- Voor bepaalde vragen of toepassingen kunnen *regulatory sandboxes* worden opgezet. Hierop kunnen partijen zich met een ontwikkelplan aanmelden.
- De competente autoriteit houdt toezicht op de *regulatory sandbox* en heeft te allen tijde de mogelijkheid om de deelname te beëindigen.
- Voor sommige toepassingen in publiek belang biedt de AI Act in dit kader extra ruimte voor het verwerken van persoonsgegevens (artikel 54). Ontwikkeling voor onderwijstoepassingen valt hier niet onder.

Specificaties van *real-world testing* buiten *regulatory sandboxes*

- Naast *regulatory sandboxes* is het ook mogelijk om toestemming te geven voor testen in *real-world settings* (artikel 54a), als daarvoor een voldoende plan wordt aangeleverd aan de competente autoriteit.
- Hiervoor moet de ontwikkelaar van de AI-toepassing zelf een testsituatie aanleveren, dus in de praktijk zal dit vanuit consortia met onderwijsinstellingen gaan.
- In tegenstelling tot bij een *regulatory sandbox,* is hier wel informed consent nodig van alle deelnemers.

Regulatory sandbox

In een *regulatory sandbox* mogen ontwikkelaars toepassingen testen en verder ontwikkelen in "echte" situaties zonder volledige certificatie.

5. Data Governance Act: Coördineren van data-altruïsme

Data-altruïsme

- Met de DGA wordt data-altruïsme (voor juridische definitie, zie kader) gereguleerd. Met data-altruïsme wordt de praktijk bedoeld waarin een non-profit-organisatie (persoons)gegevens van datasubjecten of gegevenshouders doorgeeft aan potentiële gebruikers, die de gegevens inzetten voor doelen in het algemeen belang. De datasubjecten/gegevenshouders hebben vooraf toestemming gegeven voor het gebruik van hun gegevens onder bepaalde voorwaarden.
- Lidstaten wijzen een of meer autoriteiten aan die verantwoordelijk zijn voor het registreren van erkende data-altruïsmediensten, in een openbaar nationaal register. Organisaties kunnen zich bij de betreffende autoriteit aanmelden om erkend te worden als organisatie voor data-altruïsme.
- In de DGA worden basisvoorwaarden neergelegd voor data-altruïsme. De Commissie komt hiervoor met een *rulebook* waarin de voorwaarden (zowel technisch als legaal) uiteen worden gezet, met stappenplannen voor communicatie en aanbevelingen voor interoperabiliteitsnormen. Daarnaast stelt de Commissie een Europees toestemmingsformulier op waarmee een datasubject toestemming kan geven voor gegevens.
- Verder stimuleringsbeleid kan op nationaal niveau gemaakt worden (artikel 16).

Kansen voor data-altruïsme in onderzoek

- Een organisatie die data-altruïsme voor onderzoeksdoeleinden faciliteert kan daarmee werving van respondenten en het delen van persoonsgegevens gemakkelijker maken voor onderzoekers. Momenteel moet vaak een toestemmingsverklaring worden getekend en een route voor gegevensuitwisseling worden vastgesteld indien onderzoekers gegevens willen gebruiken. Met een goed georganiseerde procedure van data-altruïsme kan de toestemmingsverklaring op voorhand geregeld zijn en kan de overdracht gestandaardiseerd zijn.
- Om data-altruïsme zo gemakkelijk en effectief mogelijk in te richten kan het waardevol zijn om dit nationaal te coördineren, zodat het voor datasubjecten makkelijk is om hun data voor zoveel mogelijk onderzoeken beschikbaar te maken en zodat het voor onderzoekers makkelijk is om zo veel mogelijk data te verkrijgen.

Artikel 2 lid 17. Definitie van data-altruïsme
17. het vrijwillig delen van gegevens op basis van de toestemming van datasubjecten om persoonsgegevens die op hen betrekking hebben te verwerken, of op basis van de toelating van gegevenshouders om hun niet-persoonsgebonden gegevens te gebruiken zonder een vergoeding te vragen of te ontvangen die verder gaat dan vergoeding van de kosten die zij maken indien zij hun gegevens beschikbaar stellen voor doeleinden van algemeen belang zoals in voorkomend geval bepaald in het nationale recht, zoals gezondheidszorg, de strijd tegen klimaatverandering, verbetering van mobiliteit, facilitering van de ontwikkeling, productie en verspreiding van officiële statistieken, verbetering van openbare diensten, openbare besluitvorming of wetenschappelijk onderzoek in het algemeen belang;

6. Data Act: Interoperabiliteit van dataverwerkingsdiensten

Interoperabiliteitseisen dataverwerkingsdiensten

- Er zijn zorgen over een vendor lock-in bij dataverwerkingsdiensten (definitie, zie rechts). Deze vragen hoge kosten voor overdracht naar andere diensten en hebben een belang om toegang tot gegevens volgens eigen (in tegenstelling tot universele) standaarden te houden.
- Met hoofdstuk 6 van de Data Act wordt gepoogd om de afnemer van deze diensten hier meer controle in te geven.
- Concreet gaat het om de volgende maatregelen:
  - Aanbieders van dataverwerkingsdiensten moeten in contracten opnemen dat ze assisteren bij de overdracht van gegevens naar een andere clouddienst op verzoek van de klant en binnen 30 dagen.
  - Vanaf drie jaar na inwerkingtreding van de Data Act moet deze overdracht gratis zijn en tot die tijd maximaal de daadwerkelijke kostprijs.
  - De leverancier van de dataverwerkingsdienst moet voldoen aan geldende Europese interoperabiliteitsnormen (opgesteld door de EC) in hun vakgebied en als die er niet zijn een export kunnen maken voor hun klanten.

Impact op afnemers van dataverwerkingsdiensten

- De impact van deze interoperabiliteitseisen zal naar verwachting substantieel zijn voor het OCW-vakgebied (en daarbuiten) voor wat betreft de controle over waar zij hun dataverwerkingsdiensten afnemen.
- Deze impact ligt op verschillende vlakken:
  - De verwachting is dat de kosten hiervoor afnemen met de toenemende interoperabiliteit.
  - De afnemer heeft zelf betere toegang tot de gegevens en kan er dus zelf ook meer waarde uit halen, omdat toegang ertoe via universele wegen mogelijk wordt.
  - Interoperabiliteit zal niet toenemen bij bijvoorbeeld digitale lesmiddelen, omdat dat een dienst is waarbij inhoud relevant is (zie het kader rechts). Wanneer het bestandsmanagement (dus bijvoorbeeld Sharepoint) betreft moet interoperabiliteit wel toenemen.

Dataverwerkingsdiensten

In grote lijnen betreft dit alle diensten die data bewaren en toegang op afstand toestaan. Daarmee kan het bijvoorbeeld ook de *hosting* van software dekken.

De bedoeling is dat het alle diensten dekt waarbij de inhoud van de gehoste gegevens/software/verwerkingen irrelevant is voor de dienst.

Ter illustratie:

- Een Elektronische Leeromgeving is een dienst om een onderwijsomgeving te bieden waarin docent en student kunnen interacteren. Hierbij doet vorm en inhoud van de gegevens ertoe en het valt er daarom niet onder, tenzij de EC anders beslist.
- Wanneer de school dit als software inkoopt en ergens laat hosten valt de hosting er wel onder: De leverancier van de hosting moet overdracht naar een andere hostingdienst faciliteren.

Aanbevelingen

Uit de gesignaleerde aandachtspunten volgen drie aanbevelingen voor het ministerie van OCW:

1. **Besteed aandacht aan de vraag of en wanneer diensten van onderwijs- en onderzoeksorganisaties ook aangemerkt kunnen worden als tussenhandelsdiensten.** Wij kunnen op basis van dit onderzoek niet met zekerheid zeggen of diensten in het kader van onderwijs en onderzoek juridisch ook als tussenhandelsdienst kunnen kwalificeren. Uit verschillende bepalingen blijkt namelijk dat de verordening is geschreven met economische activiteiten in het hoofd, en het moet gaan om 'diensten van de informatiemaatschappij', maar wanneer diensten van onderwijs- en onderzoeksorganisaties hier ook onder vallen is op basis van dit onderzoek niet helder. Zie hiervoor aandachtspunt 1. Als de DSA op deze diensten van toepassing is, kan dit leiden tot significante administratieve lasten voor onderwijs- en onderzoeksinstellingen, zie aandachtspunt 2.

2. **Besteed aandacht aan de positie van AI-systemen voor onderwijs in de AI Act.** Veel AI-toepassingen met betrekking op onderwijs vallen in het huidige voorstel onder hoogrisicosystemen. Hoewel hier goede redenen voor zijn, kan dit een beperkend effect hebben op de innovatie en toepassing van deze systemen, zie aandachtspunt 4. Voor sommige andere toepassingsgebieden op de hoogrisicolijst is extra ruimte voor innovatie gecreëerd binnen de *regulatory sandboxes*, maar voor onderwijs niet. Het zou wenselijk kunnen zijn om dit ook voor onderwijstoepassingen mogelijk te maken.

3. **Overweeg om data-altruïsme nationaal te coördineren.** Met data-altruïsme kunnen onderzoeksgegevens systematisch ter beschikking worden gesteld aan onderzoekers, met toestemming voor verwerking in het kader van (wetenschappelijk) onderzoek, via erkende en gereguleerde non-profit-organisaties. Dit kan de beschikbaarheid van data vergroten en zorgen op privacygebied bij onderzoekers wegnemen. De Digital Governance Act reguleert dit. Om data-altruïsme zo effectief en efficiënt mogelijk in te richten valt te overwegen om dit nationaal te coördineren. Zie ook aandachtspunt 5.

Dialogic innovatie & interactie
Hooghiemstraplein 33 – 36
3515 AX Utrecht
030 215 0580
info@dialogic.nl
www.dialogic.nl