Ministerie van Economische Zaken
en Klimaat

> Retouradres Postbus 20401 2500 EK Den Haag

De Voorzitter van de Eerste Kamer
der Staten-Generaal
Kazernestraat 52
2514 CV DEN HAAG

Directie Europese en Internationale Zaken

Bezoekadres
Bezuidenhoutseweg 73
2594 AC Den Haag

Postadres
Postbus 20401
2500 EK Den Haag

Overheidsidentificatienr
00000001003214369000

T 070 379 8911 (algemeen)
F 070 378 6100 (algemeen)
www.rijksoverheid.nl/ezk

Datum 23 november 2022
Betreft Geannoteerde agenda formele Telecomraad 6 december 2022

Ons kenmerk
DEIZ / 22553050

Bijlage(n)
1

Geachte Voorzitter,

Op 6 december 2022 vindt de formele Telecomraad plaats. Bijgevoegd bij deze brief vindt u, mede namens de staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties, de geannoteerde agenda met daarin een beschrijving van de discussiepunten en de Nederlandse inzet hiervoor. Middels de geannoteerde agenda wordt tevens gehoor gegeven aan het informatieverzoek van de vaste commissie Digitale Zaken van de Tweede Kamer om verdere toelichting op de AI-verordening (kenmerk: 2022Z21428).

M.A.M. Adriaansens
Minister van Economische Zaken en Klimaat

Directie Europese en Internationale Zaken

Ons kenmerk
DEIZ / 22553050

Artificial Intelligence Act
Algemene oriëntatie

Tijdens de Telecomraad ligt een algemene oriëntatie over de Artificial Intelligence Act (hierna: de AI-verordening) voor aan de lidstaten. Dit is de tekst die het mandaat vormt voor de onderhandelingen met het Europees Parlement. Het kabinet is voornemens akkoord te gaan met de voorliggende tekst.

De AI-verordening is op 21 april 2021 door de Europese Commissie gepubliceerd. De wetgeving heeft als doel om ervoor te zorgen dat er veilige AI-systemen op de interne markt komen met waarborgen voor de bescherming van fundamentele rechten. Als het Europees Parlement een positie heeft ingenomen, starten de onderhandelingen tussen de Europese Commissie, de Raad en het Europees Parlement (triloog) om tot een definitieve tekst van de AI-verordening te komen.

Zoals destijds aangegeven in het BNC-fiche, staat het kabinet positief tegenover geharmoniseerde verplichtingen voor hoog-risico AI-systemen om de ontwikkeling van betrouwbare en veilige AI te bevorderen.[1] In de geannoteerde agenda voor de Telecomraad van 3 juni 2022 is uw Kamer op de hoogte gebracht van het kabinetsstandpunt en lopende discussies tussen de lidstaten.[2] Sindsdien is het kabinetsstandpunt over de AI-verordening verder ontwikkeld, onder meer door een MKB-toets uit te voeren. Zoals toegezegd ontvangt u als bijlage bij deze geannoteerde agenda het verslag van dit panelgesprek.

Het leeuwendeel van de punten uit de kabinetsinzet is overgenomen in het Raadsakkoord, onder meer op het gebied van de definitie van een AI-systeem en daarmee de reikwijdte van de AI-verordening, het versterken van innovatie, het vergroten van transparantie en de bescherming van mensenrechten . Op verzoek van Nederland is onder andere het leereffect van *regulatory sandboxes* verstevigd, is er een registratieplicht voor overheden als gebruiker van hoog-risico AI toegevoegd, kunnen natuurlijke personen en organisaties gebruik maken van een klachtrecht en moeten fundamentele rechten worden meegenomen in de risicoanalyse voor hoog-risico AI-systemen. Hieronder wordt op deze aspecten ingegaan en op de door uw Kamer gedane verzoeken om nadere toelichting over bepaalde voor Nederland belangrijke aspecten van de AI-verordening.

De definitie van AI-systeem in het Raadsakkoord omvat naar het oordeel van het kabinet een voldoende breed scala aan AI-toepassingen. Ook AI-systemen die worden ingezet voor het bepalen van de legitimiteit van ontvangers van toeslagen of andere sociale voorzieningen (*essential public benefits*) zijn in de hoog-risico lijst opgenomen.

Hoog-risico AI systemen in het algemeen moeten aan een set vereisten voldoen voordat ze op de markt worden gebracht of in gebruik mogen worden genomen. Zo moet er onder andere een risicomanagementsysteem zijn, moet trainingsdata aan bepaalde eisen voldoen, moet er technische documentatie opgesteld worden, moet bijgehouden worden hoe het AI-systeem in de praktijk werkt ('logs'),

[1] Kamerstuk 22112, nr. 3129
[2] Kamerstuk 50133, nr. 931

moeten er gebruikersinstructies opgesteld worden en moet er menselijk toezicht zijn bij het gebruik van een AI-systeem. Ook moet het AI-systeem voldoende accuraat, robuust en cyberveilig zijn, afhankelijk van de gebruikscontext. Voor een AI-systeem dat als veiligheidscomponent in kritieke infrastructuur wordt ingezet, wordt bijvoorbeeld een hoger niveau van cybersecurity vereist.
De bescherming van mensenrechten is verstevigd door de verplichting om mogelijke risico's op schending van fundamentele rechten in de verplichte risicoanalyse voor elk hoog-risico AI-systeem expliciet mee te nemen.

Op het gebied van innovatie is de *regulatory sandbox* verstevigd waardoor bedrijven, toezichthouders en wetgevers beter kunnen leren van de ervaringen in deze innovatie- en testruimte. Om de transparantie van het gebruik van AI-systemen te vergroten is voor overheden een plicht opgenomen om hun gebruik van hoog-risico AI-systemen te registreren in de EU databank. Ten slotte hebben personen en organisaties de mogelijkheid gekregen om een klacht in te dienen bij een toezichthouder als ze vermoeden dat er een inbreuk op de AI-verordening plaatsvindt.

Voor biometrische categorisatie systemen en emotieherkenningssystemen gelden aanvullende eisen. Natuurlijke personen die aan deze AI-systemen worden blootgesteld moeten hierover geïnformeerd worden door de gebruiker van het betreffende systeem. Voor gemanipuleerde inhoud, waaronder deepfakes, moeten de makers hiervan openbaren dat het gaat om gemanipuleerde inhoud. Wat betreft het gebruik van biometrische identificatiesystemen door de rechtshandhaving is het coalitieakkoord leidend geweest bij de kabinetsinzet. Het kabinet wil niet dat deze systemen worden ingezet zonder strenge wettelijke afbakening en controle. De huidige tekst voor het Raadsakkoord bevat bovenop het bestaande wettelijke kader een verbod op het real time gebruik van deze systemen door de rechtshandhaving in de publieke ruimte waarbij een aantal uitzonderingen is geformuleerd. Deze uitzonderingen dienen nationaal bij wet te worden geregeld waardoor parlementaire controle mogelijk wordt gemaakt.

Daarnaast bevat de compromistekst een mogelijkheid om af te wijken van de reguliere procedure van conformiteitsbeoordeling zodat bepaalde AI-systemen al voor de afronding van deze procedure ingezet kunnen worden in uitzonderlijke gevallen ten behoeve van de publieke veiligheid of het leven of de gezondheid van personen, milieubescherming of voor de bescherming van kritieke infrastructuur. In de meeste gevallen dient de afwijking van deze procedure goedgekeurd te worden door de markttoezichthouder wanneer deze van mening is dat aan de eisen uit de verordening wordt voldaan.

In de motie Leijten/Rajkowski (21 501-33, nr. 935) is de regering verzocht om tijdens de onderhandelingen op wetgevingspakketten op digitale onderwerpen in te brengen dat nationaal toezicht op en/of nationale toepassing van algoritmen mogelijk moet zijn. Nederland heeft zich actief ingezet voor toezicht op nationaal niveau voor de AI-verordening. In de huidige compromistekst is opgenomen dat er op nationaal niveau één of meerdere toezichthouders worden aangewezen om toezicht te houden op naleving van de verplichtingen uit de verordening. Op Europees niveau wordt een AI Board ingesteld waarin de lidstaten zijn

vertegenwoordigd. De AI Board ondersteunt het toezicht in grensoverschrijdende gevallen, biedt een platform voor belanghebbenden en kan advies geven over de uitleg en toepassing van de AI-verordening. Daarnaast heeft Nederland zich tijdens de onderhandelingen in de Raad succesvol ingezet om te verduidelijken dat er nationale ruimte blijft voor nationale afwegingen over het gebruik van AI-systemen.

In de motie Bouchallikh/Dekker-Abdulaziz (26643, nr. 835) is de regering verzocht om te verplichten het impact assessment voor mensenrechten en algoritmen (IAMA) te doen, voorafgaand aan het gebruik van algoritmen wanneer algoritmen worden ingezet om evaluaties van of beslissingen over mensen te maken. Het verplichten van een impact assessment zoals het IAMA dient in samenhang te worden bezien met de nieuwe verplichtingen die volgen vanuit de AI-verordening. Zoals hierboven is gezegd is de bescherming van mensenrechten verstevigd door de verplichting om mogelijke risico's op schending van fundamentele rechten in de verplichte risicoanalyse voor elk hoog-risico AI-systeem expliciet mee te nemen.

In de motie Van Baarle c.s. (26643, nr. 877) is de regering verzocht om zo spoedig mogelijk een wetsvoorstel naar de Kamer te sturen waarin de overheid en bedrijven verplicht worden gesteld om concrete waarborgen te hanteren, zowel in de ontwikkelfase als in de implementatiefase, om discriminatie door algoritmen te voorkomen. In de motie Van Baarle (26643, nr. 879) is de regering verzocht om zich er in Europees verband voor in te spannen dat EU-verordeningen concrete antidiscriminatiebepalingen krijgen. Nederland heeft zich er in Europees verband actief voor ingezet dat er alleen AI-systemen op de markt komen die fundamentele rechten en dus ook de non-discriminatiebeginselen respecteren. Het kabinet heeft in de onderhandelingen over de voorgestelde AI-verordening scherp opgelet dat die rechten voldoende worden geborgd. In het Raadsakkoord staat ook steviger dat mogelijke vooroordelen in data die bijvoorbeeld tot discriminatie kunnen leiden moeten worden geïdentificeerd en voorkomen.

Raamwerk voor een Europese digitale identiteit
Algemene oriëntatie

Tijdens de Telecomraad ligt een algemene oriëntatie over het wetsvoorstel voor een raamwerk voor een Europese Digitale Identiteit (herziening eIDAS-verordening) voor aan de lidstaten.[3] De Commissie heeft dit wetsvoorstel op 3 juni 2021 ingediend ter herziening van de huidige eIDAS-verordening uit 2014.[4] Het BNC-fiche met de Nederlandse inzet is op 9 juli 2021 naar uw Kamer gestuurd.[5]

Op 3 december 2021 heeft het voorzitterschap tijdens de informele Telecomraad een voortgangsrapportage gepresenteerd, waarvan de Raad kennis heeft

[3] Voorstel voor een Verordening van het Europees parlement en de Raad van de Europese Unie, amendement op Verordening (EU) No 910/2014 betreffende de invoering van een raamwerk voor een Europese Digitale Identiteit van 3 juni 2021. COM (2021) 281, 2021/0136 (COD); C(2021) 3968.
[4] Verordening (EU) 910/2014.
[5] Kamerstuk 22 112, nr. 3161.

genomen.[6] Op 3 juni 2022 heeft het voorzitterschap in de formele Telecomraad opnieuw een voortgangsrapportage gepresenteerd, waarop enkele lidstaten, waaronder Nederland, geïntervenieerd hebben.[7]

Naar verwachting zal het meest recente compromistekstvoorstel gesteund worden door de meerderheid van de lidstaten. Nederland heeft een groot deel van de inzet binnengehaald en is voornemens in te stemmen met het Raadsakkoord.

De roep om gebruik van één uniek en persistent persoonsnummer in de Europese Unie om te borgen dat personen betrouwbaar kunnen worden gekoppeld aan wallets, leverde een spanning op tussen lidstaten die opteren voor Europese uitwisseling van één persoonsnummer, en lidstaten, waaronder Nederland, die aandacht hebben gevraagd voor de risico's hiervan en opteren voor alternatieven om personen te kunnen koppelen aan administraties (record matching). Conform de Nederlandse inzet bevat de compromistekst voldoende mogelijkheden om te werken met alternatieven voor één Europees BSN. Dit is in lijn met de manier waarop Nederland nu grensoverschrijdende identificatie onder eIDAS toestaat met meerdere persoonsnummers en pseudoniemen en in lijn met de motie van uw Kamer om deze praktijk in het voorstel te bestendigen.[8]

Wat betreft het vereiste niveau van betrouwbaarheid (level of assurance), heeft Nederland ingezet op een balans tussen een hoge mate van zekerheid over iemands identiteit enerzijds en de mogelijkheden om de wallet breed en eenvoudig te kunnen gebruiken anderzijds. Met het uiteindelijke compromis kan worden ingestemd. Wallets dienen uitgegeven te worden met een goedgekeurd eID-middel op het hoogste betrouwbaarheidsniveau. Voor landen die – anders dan Nederland – daar geen beschikking over hebben, is het mogelijk wallets uit te geven met een eID-middel op het lagere betrouwbaarheidsniveau substantieel, mits in het uitgifteproces aanvullende maatregelen worden genomen om te komen tot dezelfde mate van zekerheid over iemands identiteit als bij uitgifte met eID-middelen op het hoogste betrouwbaarheidsniveau. Welke aanvullende maatregelen toelaatbaar zij bepalen de lidstaten zelf in uitvoeringshandelingen.

In de compromistekst is de implementatietermijn voor lidstaten voor uitgifte van wallets, in lijn met de Nederlandse inzet, verlengd, en wel van 12 maanden na inwerkingtreding van het voorstel naar 24 maanden na inwerkingtreding van de relevante uitvoeringshandelingen.

De notie dat het gebruik van de wallet vrijwillig zou moeten zijn is onderdeel van het Raadsakkoord. In lijn met de moties van Uw Kamer, zal het Kabinet nationaal ook regelen dat gebruik van de digital wallet te allen tijde vrijwillig is en niemand zonder wallet geweigerd mag worden tot online overheidsdiensten of de publieke ruimte.[9] Voor het door Nederland gewenste verbod op verhandeling van gegevens van gebruikers regelt het Raadsakkoord het volgende. De afgevers van wallets

[6] Kamerstuk 21 501-33, nr. 900.
[7] Kamerstuk 21 501-33, nr. 944.
[8] Motie van het lid Ceder c.s. van 2 juni 2022, Kamerstuk 21 501-33, nr. 933.
[9] Motie van Van Baarle c.s., Kamerstuk 26 643, nr. 828, en motie van Van Haga en Leijten van 29 maart 2022, Kamerstukken 26 643, nr. 831.

mogen geen informatie over het gebruik van wallets verzamelen en mogen opgeslagen persoonsgegevens en gebruiksgegevens niet combineren met persoonsgegevens van andere diensten, indien dat niet noodzakelijk is voor het leveren van wallet diensten, tenzij de gebruiker daar zelf uitdrukkelijk om heeft gevraagd. Verder is de Algemene verordening gegevensbescherming (AVG)[10] van toepassing op ongeoorloofde, niet-noodzakelijke gegevensverwerkingen. Het is belangrijk om het verhandelverbod nadrukkelijk mee te nemen in de nationale implementatie van de verordening en bij de door Nederland uit te geven wallet. Zoals dat ook in de Wet digitale overheid gebeurd is voor eIDs, zal voor Nederlandse wallets expliciet geregeld dienen te worden dat het niet is toegestaan om persoonsgegevens te gebruiken voor andere doeleinden dan waarvoor ze verkregen zijn.

Op initiatief van Nederland is in de compromistekst een overweging opgenomen voor lidstaten om de source code van de wallet te publiceren, hetgeen tegemoet komt aan de motie van uw Kamer.[11] Door de publieke voorbeeldwallet open source te ontwikkelen, geven we dit in Nederland handen en voeten.

Ten aanzien van vertrouwensdiensten is Nederland positief over de toevoeging van nieuwe gekwalificeerde vertrouwensdiensten, de verplichte acceptatie door browsers van gekwalificeerde certificaten en de verplichting richting de Commissie om binnen 12 maanden met relevante uitvoeringswetgeving te komen. Nederland is ook succesvol geweest in het behouden van het huidige sterke toezicht op vertrouwensdiensten. Ook is er voor de nieuwe vertrouwensdienst 'elektronische attestaties van attributen' - die essentieel is voor de werking van de Wallet - een sterk toezicht vastgelegd in lijn met de Nederlandse inzet.

Dataverordening
Voortgangsrapportage

Het voorzitterschap zal tijdens de Telecomraad een voortgangsrapportage over de Dataverordening presenteren. De Dataverordening is op 23 februari jl. door de Commissie gepubliceerd. Het voorstel beoogt het gebruik van data te bevorderen, burgers en bedrijven meer controle over hun data te geven en te verzekeren dat de waarde uit data gelijkwaardiger wordt verdeeld over de partijen die deelnemen aan de data-economie. Het BNC-fiche met de kabinetsreactie op deze verordening is op 1 april jl. met uw Kamer gedeeld.[12] Het verslag van een schriftelijk overleg hierover heeft u op 17 mei 2022 ontvangen.[13]

Het kabinet is overwegend positief over het voorstel en de progressie die de afgelopen maanden onder het Tsjechische voorzitterschap is geboekt. De voortgangsrapportage van het voorzitterschap geeft weer op welke punten het voorstel de afgelopen maanden verder is aangescherpt. Belangrijke verbeteringen zijn met name dat de bevoegdheid om persoonsgegevens op te vragen in gevallen

[10] Verordening (EU) 2016/679.
[11] Motie van de leden Ceder en Dekker-Abdulaziz van 2 juni 2022, Kamerstuk 21 501-33, nr. 932.
[12] Kamerstuk 22 112, nr. 3395
[13] Kamerstuk 22 112, nr. 3411

van uitzonderlijke noodzaak is versmald en dat de verhouding met de AVG verder is verduidelijkt.

Ondanks de voortgang die is geboekt zijn er in de ogen van het kabinet een aantal belangrijke punten die verdere discussie behoeven en zijn er onderdelen van het voorstel nog onduidelijk. Het gaat daarbij met name om de bevoegdheid voor overheden om gegevens op te vragen in gevallen van uitzonderlijke noodzaak en het bevorderen van de interoperabiliteit van clouddiensten.

Hoewel de bevoegdheid voor overheden om gegevens op te vragen in gevallen van uitzonderlijke noodzaak is vernauwd, blijft het kabinet hier aandacht voor houden. Het kabinet blijft zich inzetten om de bevoegdheid van aanvullende waarborgen te voorzien en verder te versmallen. Het draagvlak bij andere lidstaten en Commissie voor verdere inperking van de bevoegdheid is overigens beperkt.

Over maatregelen die overstappen tussen clouddiensten beter mogelijk maken is het kabinet positief. Het kabinet zet zich in dat in aanvulling hierop ook maatregelen worden genomen om de interoperabiliteit tussen clouddiensten in het algemeen te bevorderen. Het kabinet wordt hierin gesterkt door de marktstudie clouddiensten van de ACM[14]. Op basis van de marktstudie suggereert ACM om aanvullende maatregelen in de Data Act gericht op interoperabiliteit van clouddiensten op te nemen om de markt voor clouddiensten meer open, competitief en innovatief te maken. Tot slot zijn er aantal belangrijke onderdelen omtrent datadeling uit IoT-producten die het kabinet graag verder ziet verduidelijkt, waaronder belangrijke definities als ‘gebruiker’ en de bepalingen over compensatie voor datahouders.

Cyber Resilience Act
Voortgangsrapportage

De Europese Commissie heeft op 15 september jl. een voorstel gedaan voor de Cyber Resilience Act (CRA), een verordening die de cybersecurity van met internet verbonden producten regelt. De Raad is onder het Tsjechisch EU-voorzitterschap gestart met de bestudering van het voorstel op technisch niveau, en heeft al enige inhoudelijke discussie gevoerd over het toepassingsbereik van de verordening. Voor de Telecomraad staat een voortgangsrapport op de agenda waarin de stand van zaken van de behandeling in de Raad en de volgende stappen onder het inkomende Zweedse voorzitterschap vanaf januari 2023 beschreven staan. Het Zweeds EU-voorzitterschap zal onderhandelingen op de CRA voortzetten, met als ambitie een gemeenschappelijke positie van de Raad te bereiken. Het Europees Parlement is nog niet gestart met de behandeling van het CRA-voorstel.

Een eerste algemene Nederlandse positie is vastgelegd in het op 21 oktober gedeelde BNC-fiche. Vlak voor publicatie van het CRA-voorstel heeft Nederland, samen met Duitsland en Denemarken, een gedeelde positie gepubliceerd in een non-paper over de CRA. Dit non-paper is uitgebracht en verspreid in Brussel.[15]

[14] Marktstudie clouddiensten | ACM.nl
[15] Dit non-paper is ook met de Tweede Kamer gedeeld, Kamerstukken, 2021-2022, 22 112, nr. 3523.

Deze inspanningen hebben effect geresulteerd. Het voorliggende Commissievoorstel komt in grote mate tegemoet aan de wensen van Nederland. Het kabinet verwelkomt horizontale EU-wetgeving die de cybersecurity van alle producten met digitale elementen regelt en daarmee de Europese digitale interne markt veiliger en beter functionerend maakt: tot dusver was er alleen sectorale EU-wetgeving die de cybersecurity van een beperkt aantal specifieke producten en diensten reguleerde. Voor het kabinet is het waarborgen van cybersecurity gedurende de productlevenscyclus belangrijk. Het kabinet wil daarom meer duidelijkheid over het voorstel van de Commissie om de termijn hiervoor te beperken tot maximaal vijf jaar, of de gehele levenscyclus van het product als die korter is. Voor het kabinet is het verder belangrijk dat de definities en reikwijdte helder zijn. Ook moet voldoende inzichtelijk zijn hoe de CRA met andere wetgeving samenhangt, zoals de herziene Netwerk- en informatiebeveiligingsrichtlijn (NIB-2) en de Cyber Security Act. Daarnaast zal het kabinet de Commissie vragen om de redenen voor het niet meenemen van digitale dienstverlening onder de verordening. Het kabinet heeft daarnaast in het CRA oog voor de administratieve lasten die het voorstel meebrengt, en het bieden van juridische zekerheid aan bedrijven. Tot slot kijkt het kabinet scherp naar nieuwe rol en bevoegdheden voor de Europese Commissie en het Agentschap van de EU voor cyberbeveiliging (ENISA), bijvoorbeeld in relatie tot de nationale veiligheid. Die bevoegdheden zien onder meer op het in uitzonderlijke omstandigheden kunnen weren van producten van de markt door de Commissie, of het instellen van een meldplicht voor producenten bij geëxploiteerde kwetsbaarheden bij ENISA.

Digitale vaardigheden in het digitale decennium
Beleidsdebat

Het voorzitterschap is voornemens een beleidsdebat te voeren over '*digital skills in the digital decade*'. Er is nog geen agenda beschikbaar. Het is gunstig dat de Commissie dit onderwerp agendeert. Nederland is één van de Europese koplopers op digitale vaardigheden, hetgeen bijdraagt aan onze internationale concurrentiepositie. Tegelijkertijd bestaan er een aantal belangrijke aandachtspunten. De inbreng van Nederland zal langs onderstaande lijnen zijn.

Allereerst vindt het kabinet het belangrijk dat iedereen mee kan doen. Het kabinet verwelkomt dan ook de EU doelstelling dat 80% van de Europese bevolking in 2030 over digitale basisvaardigheden moet beschikken.[16] In de DESI-index heeft 79% van de volwassen Nederlanders digitale basisvaardigheden. Nederland is een van de best presterende EU-landen op het gebied van digitale vaardigheden en menselijk kapitaal (plek 2 DESI index). Nederland behoort ook tot de top vijf van EU landen wat betreft het aandeel van ICT-specialisten als percentage van de beroepsbevolking. Toch heeft Nederland nog veel meer ICT-specialisten nodig om koploper in de digitale transitie te blijven. Het percentage afgestudeerde ICT'ers in Nederland (3,4 %) blijft bovendien achter bij het EU-gemiddelde van 3,9 %. Het kabinet zet daarom met de Werkagenda Waardengedreven Digitalisering, het Masterplan Basisvaardigheden, de Strategie Digitale Economie en het Actieplan

[16] Tweede Kamer, 2021-2022, 22 112, nr. 3238.

Groene en Digitale banen in op digitale vaardigheden bij alle Nederlanders; ook diegenen die de basis al kennen. Het kabinet vindt dat in de eerste plaats het bedrijfsleven als eerste verantwoordelijke en vervolgens de nationale overheden (in plaats van de EU) aan zet zijn om de randvoorwaarden te realiseren voor het verhogen van het aantal ICT'ers. In Nederland wordt daarom een actieplan groene en digitale banen ontwikkeld waarmee het kabinet extra inzet wil plegen op het vraagstuk van arbeidskrapte voor de klimaat- en digitale transities. Er is daarnaast specifieke aandacht voor het verbeteren van de *kritische* digitale vaardigheden, zoals op desinformatie en delen van data. We blijven de digitale basisvaardigheden van burgers verbeteren met het programma Tel Mee Met Taal. Daarnaast streeft Nederland er naar dat ook alle kinderen digitaal vaardig van school af gaan. Nederland zal de komende jaren digitale vaardigheden verder verankeren in het formele curriculum.

In de 'gestructureerde dialoog' met de lidstaten over digitaal onderwijs en vaardigheden heeft de Commissie dit jaar aandacht gevraagd voor de bijdrage vanuit het onderwijs, het nationale beleid, de rol van het bedrijfsleven en sociale partners en de verschillende benaderingen gericht op basis- en meer geavanceerde digitale vaardigheden. Door de coherentie te bevorderen tussen beleidsterreinen kunnen de EU-doelstellingen voor 2030 beter worden gerealiseerd. Het kabinet heeft eerder dit initiatief tot uitwisseling van ervaringen tussen lidstaten verwelkomd,[17] en hoopt in dit beleidsdebat ook van de Commissie de resultaten daarvan te horen. Dit ook met het oog op de volgend jaar aangekondigde voorstellen door de Commissie op het gebied van digitaal onderwijs en onderwijs en training in digitale vaardigheden[18] en het Jaar van de Vaardigheden 2023 waarin ook extra aandacht voor om- en bijscholing in digitale vaardigheden zal zijn. Het Europees Parlement heeft eerder dit jaar in haar reactie op het Commissievoorstel voor het beleidsprogramma Digitaal Decennium de ook door de Raad overgenomen Europese doelstelling m.b.t. digitale basisvaardigheden geheel ondersteund.[19]

Diversenpunten
Het voorzitterschap zal een update geven van de onderhandelingen met het Europees Parlement overlopende EU-voorstellen waaronder ePrivacyverordening. Verder zal het voorzitterschap een update geven over de Verklaring over digitale rechten en beginselen en een terugkoppeling geven over de high-level expert bijeenkomst over governance en handhaving van EU regelgeving in de digitale omgeving en over de Conferentie over een veilige en innovatieve digitale toekomst van de EU. De Commissie zal over Telecomsteun aan Oekraïne en een update geven over internationale initiatieven over digitalisering, met een focus op de EU-VS Trade & Technology Council (TTC) en Digitale partnerschappen). Tot slot zal Zweden het voorzitterschapsprogramma van januari - juni 2023 presenteren.

Verklaring over Europese Digitale Rechten en Beginselen

[17] Staat van de Unie 2022, Tweede Kamer 2021-2022, 35 982, nr. 3.
[18] Zie afschrift van de Nederlandse reactie op de consultatie via Raad voor Onderwijs, Jeugd, Cultuur en Sport | Tweede Kamer der Staten-Generaal
[19] REPORT on the proposal for a decision of the European Parliament and of the Council establishing the 2030 Policy Programme "Path to the Digital Decade" | A9-0159/2022 | European Parliament (europa.eu)

De Europese Commissie heeft begin dit jaar een conceptverklaring over Digitale Rechten en Beginselen voor het Digitale Decennium gepresenteerd.
Het BNC-fiche met de kabinetsreactie op deze verklaring is op 18 maart 2021 met uw Kamer gedeeld.[20] Het BNC-fiche bevat een positieve grondhouding: de verklaring benadrukt een digitale transformatie, waarin de mens centraal staat en waar prioriteit wordt gehecht aan het versterken van de rechten en vrijheden in het digitale domein.

Het voorzitterschap stuurt op snelle afronding van de interinstitutionele besprekingen. Het voorstel is in lijn met bovenstaand Nederlands standpunt. Nederland heeft onder andere het belang van regelmatig monitoren van de voortgang met betrekking tot in hoeverre de Europese waarden worden nageleefd richting de Raad en het Parlement onderstreept. De EU-lidstaten zitten goed op één lijn. Een groot aantal lidstaten pleit voor een verwijzing naar universele mensenrechten en benadrukt dat de verklaring in lijn moet zijn met (lopende) wetgevingsvoorstellen.

[20] Kamerstuk 22112, nr. 3347, https://zoek.officielebekendmakingen.nl/kst-22112-3347.html.

Verslag MKB toets AI Act d.d. 22 september 2022

Het panel bestond uit diverse vertegenwoordigers van het MKB, zowel mannen als vrouwen. Er waren consultants die het MKB adviseren, maar ook zelf AI-systemen bouwen voor het MKB. Er waren mensen die zelf voor een MKB werken en mensen die in startups investeren. De indruk is dat de bijeenkomst mede werd beschouwd als goede gelegenheid om geïnformeerd te worden.

Er waren vooraf enkele vragen gesteld over het voldoen aan de eisen:

1. Is het duidelijk wanneer een systeem in de categorie hoog-risico valt?
2. Zijn de verplichtingen duidelijk waaraan het systeem in dat geval moet voldoen?
3. Zo nee, Wat heb je nodig? Welke informatie mis je om deze stappen wel te doorlopen?
4. Op welke manier zouden MKB-ers die een hoog-risico AI-systeem ontwikkelen of op de markt brengen, het beste ondersteund kunnen worden?
5. Zie je nog specifieke andere knelpunten die onze aandacht moet hebben?

Ook waren er vragen gesteld over de innovatiestimulerende maatregelen:

1. Aan welke voorlichting over de AI verordening heb je het meest behoefte?
2. Hoe werkt het testen van AI -systemen nu en wat is nodig om dat te blijven doen onder de AI verordening?
3. Wat voor begeleiding verwacht je bij deelname aan een regulatory sandbox?
4. Wat is er voor een mkb'er die hoog risico AI-systemen ontwikkelt nodig om te voorkomen dat de regeldruk door deze verordening te hoog wordt?
5. Wat voor praktische ondersteuning gaat een mkb'er in praktijk helpen door een toezichthoudende instelling? Bijv. normuitleg, handvatten voor compliance of andere onderwerpen?
6. Wat mist er?

Aan de hand van een presentatie over de AI-verordening die later is gedeeld, is het gesprek gevoerd. De presentatie riep zo veel vragen op dat er niet is toegekomen aan de vragen die op voorhand waren gedeeld. De deelnemers missen begrijpelijkerwijs nog kennis over wat de AI-verordening gaat vereisen en stelden met name vragen over wat de wet voor hen specifiek gaat betekenen.

Uit de vragen bleek veel behoefte aan uitleg over de systematiek van de AI-verordening. Zo bleken veel onduidelijkheden te zijn wat betreft de combinatie 'vallen onder de definitie van AI-systeem' wat niet direct gevolgen heeft, en 'vallen in de hoog-risico categorie', gevolgd door het moeten voldoen aan de eisen uit de AI verordening. Ook de categorie AI-systemen waar moet worden voldaan aan transparantievereisten, waren niet helder genoeg voor iedereen.

Een deel van de vragen kon nog niet worden beantwoord doordat de artikelen in de AI-verordening die daarover gaan, pas na de toets zijn besproken aan de hand van nieuwe voorstellen van het voorzitterschap, zoals de volgende:

- Wat mag een middelgroot of klein bedrijf die doet aan bewaken en beveiligen met AI?
- Een partij die namens een opdrachtgever persoonsgegevens bewerkt met behulp van AI, en die persoonsgegevens na bewerking moet vernietigen, hoe hangt dat samen met de verplichting van het bewaren van de logs? Hoe is hier de samenhang tussen de AIA en de GDPR?
- Gaat de AI-verordening ook van toepassing zijn op reeds bestaande systemen? Antwoord: alleen als er sprake is van een substantiële wijziging.
- Hoe is de situatie als een klant die het AI-systeem gebruikt je verwijt van het niet voldoen aan de vereisten van de AIA?
- Wanneer een laboratorium biologisch materiaal verwerkt en analyseert met AI om bijvoorbeeld voedingsadviezen te geven, maar dit geheel anoniem doet, valt dat dan onder hoog risico?

- Er zijn veel systemen die bijvoorbeeld *libraries* van onderliggende AI-systemen gebruiken. Dat zullen general purpose AI-systemen zijn. Wanneer een dergelijk AI systeem hoog risico is, moeten alle onderliggende systemen dan ook aan de eisen voldoen?

Uit het gesprek komt naar voren dat de voornaamste last voor het hele MKB zal zijn om te beoordelen welk risico verbonden is aan hun AI-product, d.w.z. de inspanning om te bepalen welke rol het bedrijf heeft in de context van de AI-verordening en of het AI-product een hoog-risico AI-systeem betreft of een andere categorie waar eisen aan verbonden zijn.