

Ministerie van Economische Zaken
en Klimaat

> Retouradres Postbus 20401 2500 EK Den Haag

De Voorzitter van de Tweede Kamer
der Staten-Generaal
Prinses Irenestraat 6
2595 BD DEN HAAG

**Directoraat-generaal
Economie en Digitalisering**

Bezoekadres
Bezuidenhoutseweg 73
2594 AC Den Haag

Postadres
Postbus 20401
2500 EK Den Haag

Overheidsidentificatienr
00000001003214369000

T 070 379 8911 (algemeen)
F 070 378 6011 (algemeen)
www.rijksoverheid.nl/ez

Ons kenmerk
DGED / 104522997

Uw kenmerk
22112-4223

Bijlage(n)
2

Datum 6 maart 2026
Betreft Naderend Raadscompromis Omnibus AI

Geachte Voorzitter,

Sinds de publicatie van de voorstellen voor een Omnibus AI en Omnibus Digitaal op 11 november jl. wordt in de Raad onder hoge druk onderhandeld over de hierin voorgestelde aanpassingen aan digitale wetgeving. De onderhandelingen voor de Omnibus AI bevinden zich al in een afrondende fase. Het Cypriotische voorzitterschap zal, eerder dan verwacht, waarschijnlijk tijdens de Coreper-II-bespreking van 13 maart aanstaande, het bereikte compromis aan de lidstaten voorleggen en een mandaat vragen voor de onderhandelingen met het Europees Parlement (EP).

Middels deze brief informeer ik uw Kamer conform de gemaakte informatie-afspraken over de ontwikkelingen in de onderhandelingen en hoe het kabinet het verwachte compromis op de Omnibus AI apprecieert. Eerder is uw Kamer via het BNC-fiche over de omnibussen¹ geïnformeerd over de kabinetsinzet en de voortgang van de onderhandelingen. In lijn met het parlementair behandelvoorbehoud maakt het kabinet tot na het mondeling overleg met de Eerste Kamer op 17 maart tijdens de onderhandelingen over de digitale omnibussen een voorbehoud. Het kabinet blijft met dat voorbehoud het standpunt zoals geformuleerd in het BNC-fiche uitdragen, inclusief de zorgen die daarin worden geuit.

Regeldrukvermindering is een belangrijke prioriteit van dit kabinet en de verwachte Raadspositie is grotendeels in lijn met de inzet uit het BNC-fiche. Het kabinet is dan ook positief over het verwachte onderhandelingsresultaat op de Omnibus AI. Gezien het parlementaire behandelvoorbehoud dat de Eerste Kamer heeft geplaatst bij de Omnibus AI en Omnibus Digitaal zal het kabinet echter een voorbehoud moeten maken over de Raadspositie op de Omnibus AI. Dit zou de onderhandelingspositie op beide digitale omnibussen voor de rest van de onderhandelingen kunnen verzwakken. Gezien het belang van het adresseren van de zorgen over sommige onderdelen van de Omnibus Digitaal en de positieve uitkomst van de onderhandelingen op de Omnibus AI heb ik de Eerste Kamer

¹ Kamerstukken II 2025/2026, 22112, nr. 4223

gevraagd of zij bereid is het behandelvoorbehoud op de Omnibus AI op te heffen zodat het kabinet zich positief kan uitspreken over het bereikte Raadscompromis. Indien de Eerste Kamer hier niet toe bereid zal het kabinet uiteraard conform de afspraken een voorbehoud maken over de Raadspositie op de Omnibus AI.

Omnibus AI

De onderhandelingen over de Omnibus AI zijn in een vergevorderd stadium. Tegelijkertijd is de inhoud van de concept-Raadspositie nog steeds in beweging. Zoals aangegeven in het BNC-fiche, bevatte het voorstel voor de Omnibus AI verschillende wijzigingen die het kabinet kan steunen omdat deze het voor organisaties eenvoudiger maken om aan de AI-verordening te voldoen, zonder afbreuk te doen aan de doelen van de verordening. De voorgestelde wijzigingen dragen bij aan vermindering van administratieve lasten doordat bepaalde registratieverplichtingen worden geschrapt of vereenvoudigd en meer duidelijkheid wordt geboden over verplichtingen voor organisaties die AI-systemen ontwikkelen of gebruiken. Er lijkt voldoende steun om deze wijzigingen te behouden in het Raadscompromis.

In het BNC-fiche heeft het kabinet ook aangegeven dat het op een aantal onderwerpen inzet op verbetering van het oorspronkelijke voorstel. De belangrijkste hierin zijn de aangepaste bevoegdheid voor het verwerken van bijzondere categorieën van persoonsgegevens voor biasdetectie en -correctie, het schrappen van de registratieplicht voor bepaalde AI-systemen die in hoog-risico context worden gebruikt, de aanpassingen omtrent AI-geletterdheid en uitstel van de inwerkingtreding van de bepalingen omtrent hoog-risico AI. De Raadspositie zal ten opzichte van het voorstel op al deze punten waarschijnlijk meer in lijn zijn gebracht met de kabinetspositie.

Voor de bevoegdheid voor het verwerken van bijzondere categorieën van persoonsgegevens voor biasdetectie en -correctie, lijkt er voldoende steun te zijn om deze bevoegdheid te limiteren tot verwerkingen die strikt noodzakelijk zijn voor het detecteren, corrigeren en voorkomen van bias die waarschijnlijk de gezondheid en veiligheid van personen aantast, grondrechten schaadt of tot discriminatie leidt. Dit is in lijn met het gezamenlijke advies van de Europees Comité voor Gegevensbescherming (EDPB) en de Europese Toezichthouder voor Gegevensbescherming (EDPS). Met deze aanvullende waarborgen acht het kabinet de bevoegdheid proportioneel tot het doel van detecteren en corrigeren van bias, zeker aangezien bias in AI-systemen op zichzelf ook grondrechten kan schaden.

In de Raadspositie blijft waarschijnlijk, in lijn met de kabinetspositie, de registratieplicht behouden voor AI-systemen die in hoog-risico context worden gebruikt, maar op zichzelf geen hoog risico vormen. Ook lijkt er voldoende steun om, in lijn met de kabinetsinzet, de inwerkingtreding van de bepalingen voor hoog-risico AI-systemen niet te koppelen aan besluiten van de Europese Commissie. Het kabinet heeft liever dat de inwerkingtreding van de bepalingen voor hoog-risico AI-systemen die in bijlage III van de AI-verordening zijn

opgenomen minder lang wordt uitgesteld, maar hier is onvoldoende steun voor in de Raad.

Tot slot lijkt er voldoende steun om in de aangepaste bepaling over AI-geletterdheid expliciet te maken dat aanbieders en gebruiksverantwoordelijken van AI-systemen nog steeds verantwoordelijkheden en verplichtingen hebben om voor voldoende training en vaardigheden te zorgen bij hun werknemers. Ook zullen er door de AI Raad (AI Board) aanbevelingen en niet-bindende gezamenlijke doelstellingen van lidstaten worden vastgesteld met betrekking tot AI-geletterdheid. Hiermee komt meer duidelijkheid over de implicaties van de verplichting omtrent AI-geletterdheid voor overheden en organisaties. Het kabinet zou nog verdere verduidelijking van deze verplichting verwelkomen.

Een punt waar nog discussie over is in de Raad, is de voorgestelde exclusieve bevoegdheid voor de AI Office om toezicht te houden op hoog risico AI-systemen die zijn gebaseerd op AI-modellen voor algemene doeleinden (GPAI-modellen), waarbij zowel het GPAI-model als het AI-systeem van dezelfde aanbieder zijn. Er zijn met name zorgen dat deze exclusieve bevoegdheid ertoe kan leiden dat de AI Office ook op een grote groep gebruiksverantwoordelijken van zulke AI-systemen toezicht zal moeten houden, wanneer deze vallen onder dezelfde juridische entiteit als de aanbieder. Deze groep zal in de toekomst mogelijk steeds groter worden naarmate het gebruikelijker wordt voor organisaties om GPAI modellen zelf te ontwikkelen. Deze gebruiksverantwoordelijken kunnen ook organisaties zijn met een publieke taak die raakt aan nationale competenties, zoals binnen de rechtshandhaving of de rechtspraak. Het toezicht op deze organisaties past niet onder de exclusieve bevoegdheid van de EU. Er lijkt nu voldoende steun te zijn voor aanpassingen aan deze bevoegdheid, die voorkomen dat de bevoegdheid van de AI Office botst met nationale bevoegdheden.

Het kabinet zal zich blijven inzetten om bovenstaande prioriteiten zoveel mogelijk in de Raadspositie te laten landen. Als het lukt om tot overeenstemming te komen in de Raad, zal ik uw Kamer informeren over de uitkomsten hiervan. Na totstandkoming van de Raadspositie zal het Europees Parlement nog zijn positie moeten bepalen, en volgen de trilogie om te komen tot een definitieve Omnibus AI. Het voorzitterschap streeft ernaar dat de Omnibus AI uiterlijk in augustus 2026 in werking treedt, omdat de bepalingen voor sommige hoog-risico AI-systemen 16 augustus 2026 in werking treden.

Omnibus Digitaal

De onderhandelingen over de Omnibus Digitaal zijn minder ver gevorderd dan de onderhandelingen over de Omnibus AI. Voor verschillende punten waar het kabinet zorgen heeft geuit lijkt er steun van een aantal lidstaten om deze zorgen te adresseren. Zo lijkt er steun van verschillende lidstaten om de definitie van persoonsgegevens in stand te houden en om bepaalde bepalingen in de P2B-verordening te behouden. Ook met betrekking tot de zorgen over bepaalde wijzigingen aan de AVG en het Europees centraal meldpunt zijn er meerdere lidstaten die vergelijkbare zorgen lijken te hebben. Het kabinet heeft ook samen

met andere lidstaten non-papers opgesteld over de in het BNC-fiche geuite zorgen over het Europees centraal meldpunt en de P2B-verordening. Deze non-papers zijn bijgevoegd bij deze brief.

Willemijn Aerdt
Staatssecretaris Digitale Economie en Soevereiniteit

Non paper – Digital Omnibus - Single Entry point for incident notifications

‘Towards simplifying the cybersecurity landscape, instead of adding complexity’

By France, Germany, Italy, the Netherlands, Spain and Sweden

In a world where swift action is needed to effectively counter cyber threats, simplifying the cybersecurity landscape is a necessity. The proposal of the European Commission to develop a Single-Entry Point for incident notifications at EU-level would only add more complexity to incident response and notification, impacting consequently the current processing of incident notifications at national level by Member States. We strongly believe that the Commission should find alternative ways to effectively create clarity within the landscape.

1. The pivotal role of national CSIRT's within the cyber landscape.

As cooperation and coordination between Member States are needed to effectively counter cyber threats, the most effective way to realize this is to invest in existing structures. National CSIRT's and competent authorities play a fundamental role within the cyber landscape, as they officiate as deeply entrusted partners for entities. They also dispose of profound knowledge of the sectors within each specific Member State. They are consequently best placed and equipped to help and support entities in times of cyber crises throughout the whole process, from assistance to incident notification and incident response. Indeed, incident reporting can not only be seen as a legal obligation, but should be directly linked to the role of CSIRTs to assist victims facing a cybersecurity incident. The CSIRT role is central in helping entities through assistance but also accompanying the victim in the notification process.

The trust assigned to national CSIRT's and competent authorities did not emerge overnight, but has been built steadily over the years. Their constant and pivotal implication in the landscape should not be underestimated as they helped shape strong national structures. Trust is -as widely understood- a crucial aspect in the cyber domain, as being targeted by cyber-attacks or having to deal with an important incident can be a very sensitive matter. This is especially the case for small and medium enterprises, being also the most vulnerable for cyber-attacks. The organization of incident reporting at the national level is or has been already a significant burden for these entities. Changing and restructuring incident reporting to the EU-level therefore does not only undermine the trust that was built with national CSIRT's, but also increases the administrative burden for entities. Even more, introducing this initiative could even be experienced as an encumbrance for the timely handling of cyber incidents.

2. An inadequate technical solution that would complexify the existing structures

The proposal for a Single-Entry Point constitutes a technical feature with which the Commission aims to centralise different reporting regimes at the EU level. However, until this day it remains unclear and unproven as to how this technical solution will lead to simplification and harmonization, since the necessary prerequisites are not elaborated yet.

Introducing a Single-Entry Point at EU level at this stage would lead to more complexity, given the fact that operational and efficient national structures are already in place, that national reporting obligations exist alongside European obligations and that it touches national competences. The processes related to reporting obligations should remain the sole responsibility of the Member States. Also, the majority of entities conduct their operations

within a single or a few Member States, and thus do not have cross-border operations, complexifying the process for a majority of entities without simplifying cross-border notifications.

Finally, centralizing sensitive information on incident notifications of 27 Member States would render the EU more vulnerable for cyber-attacks in the event of inadequate security measures. Bringing together in one single point all vulnerabilities of private, public and civil structures, would pose a very significant risk to the security of information systems and national security. This centralization also creates dependencies with regards to the continuity of services, since potential failure or downfall of this critical (notification) processes may have considerable consequences.

We strongly believe that the alignment and streamlining of incident notifications is part of the needed prerequisites and would directly contribute to the regulatory simplification. Working on harmonisation would support entities in navigating the administrative regulatory obligations, and Member States could integrate these into their national notification processes, enabling secure processing of the reported incident. This is the most effective way to simplify incident notification at EU level, and is a first but prerequisite step towards simplification.

3. Our solution to maximize our simplification efforts:

In addition to harmonising European incident reporting obligations and in order to further support entities navigating EU cybersecurity incident notification landscape, we see strong added value in the development of an EU website on EU-wide incident reporting obligations. This website could be developed and managed by ENISA and should help identify and connect with the most appropriate national responder, enhancing clarity and accessibility, while allowing an anonymous navigation. This European website for guidance would map all obligatory incident reporting in the different Member States and at EU level and provide links to the competent reporting authority. Developing a mapping tool of the regulatory landscape contributes to sharing knowledge and information as part of the current ENISA's mandate.

Considering all the above, we propose the first draft of compromise text should focus on the following:

The EU Single Information Point will consist of a publicly accessible website developed and managed by ENISA. The Single Information Point will reduce administrative burden for entities by providing information on reporting and assistance structures and a clear overview of information on incident reporting of the respective legislation. The Single Information Point will give a clear and centralised overview on when, where and how entities must report security incidents to the recipients defined in respective legislation. This overview may include the redirecting of Website-visitors to the respective Member States' national entry points and/or reporting forms.

There will be no changes to the respective legislation, as Member States remain the sole and direct recipient of all notifications and continue to have the sole responsibility for all processes related to reporting obligations. The Single Information Point-website will not collect any data on reports or notifications and will not store any data related to the reporting obligations following the respective legislation.

We do strongly support the Commission's objective to simplify the cyber landscape and reduce the administrative burdens for entities. This requires effort from both the European institutions and from the Member States, and better alignment of existing legislative frameworks. We believe that a first step is mapping the European and national obligations in terms of incident reporting. Next, deadlines, templates and national end-points for notification should be better aligned to improve user-friendliness. Where feasible, centralisation of national end-points for cyber notifications should be encouraged. Finally, different concepts and definitions should be harmonised and a common set of data to notify should be defined. This way, simplification efforts in the cybersecurity domain can have real added value for entities and governments alike.

Non-paper on the repeal of the P2B Regulation in the Digital omnibus

This is a joint non-paper of Austria, Belgium, Italy and the Netherlands. The signatories acknowledge and support the Commission's efforts to reduce administrative burdens by avoiding potential overlaps between the P2B Regulation and other EU legislation. Addressing those parts of the P2B Regulation that clearly overlap with other EU legislation, primarily the DSA and DMA, will simplify the applicable rules and increase legal certainty for businesses, making the EU more competitive and commercially attractive.

However, the Commission's proposal to repeal the entire P2B Regulation, with only limited and time-gated exceptions, will lead to loopholes and weaknesses in the legal protections that are disproportionate to the marginal reduction in administrative burdens that would be achieved.

While simplification efforts are supported by the signatories, they should not come at the expense of the essential safeguards for European SMEs. Such safeguards include transparency regarding general terms and conditions, predictability in the event of changes, insight into rankings and clear procedures in the event of restriction or suspension. Their importance is reflected in the growing awareness of P2B rights and the increasing number of complaints concerning non-compliant platforms.

The P2B Regulation contributes to the proper functioning of the single market by harmonising rules that afford transparency, fairness and effective redress tools to business users of platforms. In this regard, it has a specific approach and constitutes a first step toward establishing a comprehensive EU legal framework for online intermediaries. The DMA and DSA have different targets and scopes. They do not provide the same substantive obligations, nor do they offer the subsidiarity and proximity afforded by the P2B Regulation. Therefore, they cannot offer the same level of protection in such situations.

Simplification efforts should lead to a genuine reduction in regulatory burden. We believe that targeted adjustments to remove clear overlaps with the DSA and DMA would streamline the regulatory framework without dismantling essential protections. The limited administrative burden associated with the remaining P2B provisions, as detailed below, would be proportionate in light of the legal certainty and protection they afford SMEs.

Therefore, we urge the Presidency to propose a more targeted and proportionate approach to reduce complexity and administrative burdens within the P2B Regulation while preserving the necessary protection this legislation offers for businesses, in particular SMEs. Below, we set out the substantive provisions that need to be maintained to ensure an adequate level of protection for business users as well as the enforcement measures that avoid the risk of a governance gap due to weakened national enforcement. Furthermore, adequate protection of business users, particularly SMEs, should be maintained on a permanent basis.

1. Substantive provisions that should remain to ensure adequate protection for business users

a. Material obligations

Right to termination and notice period in case of changed T&C's (Article 3.2) Besides the transparency obligations discussed below, Article 3 also contains material obligations for platforms. Without Article 3.2, business users will no longer be informed before terms and conditions are changed and they will lose the right to terminate the agreement on these grounds. This harms the business user's position in their relation to the platform by weakening contractual transparency and predictability.

Notice period in case of termination (Article 4.2) The repeal of this provision would lead to business users no longer being granted a notice period before their access to the platform services is terminated. This prevents them from taking appropriate measures or challenging the termination decision before it takes effect, rendering them vulnerable to arbitrary decisions by the platform.

Complaint handling system (Article 11) The repeal of Article 11 severely limits the business user's ability to challenge unfair or illegal conduct through an internal complaint-handling system. While they will still have access to an internal complaint handling system under the DSA, its scope is limited to illegal content or alleged violations of the platform's terms and conditions. This in turn leaves the business user without quick and effective remedies against P2B non-compliance by the platform, technological issues or any other measures taken by the platform in the context of providing intermediation services that affect the business user.

b. Transparency obligations

Terms and conditions (Article 3) In addition to the material obligation of Article 3(2) mentioned above, the transparency obligations set out in Article 3 offer considerable protection to business users, particularly since non-compliant terms and conditions are automatically null and void. The repeal of Article 3 would remove an important safeguard for business users against arbitrary enforcement, thereby depriving them of the right to be informed in advance, in a clear and comprehensible manner, of the potential conditions under which the service may be restricted, irrespective of the size of the platform.

Ranking (Article 5) National authorities play a crucial role in addressing ranking-related complaints from business users, and some signatories have received a notable number of such requests under the current P2B framework. Repealing Article 5 would therefore shift the enforcement of these issues away from national regulators and risk reducing the accessibility and effectiveness of redress for SMEs operating on platforms.

Differentiated treatment (Article 7) Without this provision, platforms are free to put business users at a disadvantage where they compete with the platform's own products and services, or with other business users controlled by the platform, without disclosure. Because there is no obligation of any kind to be transparent, business users will not be able to know whether, how and why this is happening. The transparency required by Article 7 provides insight into the different forms of differentiated treatment and enables authorities, including those under the

DMA and competition law, to detect and address such practices. Again, it is important to note that some signatories have received a notable number of Article 7 complaints and tip-offs.

Parity clauses (Article 10) As most platforms are not gatekeepers, repealing Article 10 will allow them to impose parity clauses without transparency. They will not need to provide any justification and prospective business users will not know such restrictions exist. This lack of transparency will make it significantly more difficult for authorities to gain insight into these practices and for affected business users to challenge them.

2. Enforcement measures

The repeal of the P2B Regulation would also mark a shift concerning the enforcement of the rules on online platforms. Article 15 explicitly empowers Member States to enforce its provisions, ensuring proximity between the enforcement body on the one hand and the user that is protected on the other hand, in line with the principle of subsidiarity. This is in contrast to the governance frameworks under the DSA and DMA. In this regard, the P2B Regulation operates as a complementary governance instrument. Whereas the DMA establishes a centralized enforcement model for gatekeepers at Commission level, and the DSA relies predominantly on the country-of-origin principle for oversight of intermediary services, the P2B Regulation provides a more granular and business-user-focused framework enforced directly by Member States. A clear example of this can be seen in the enforcement of Articles 5 and 7 vis-à-vis non-gatekeeper platforms, whereby national enforcement bodies can take action against unfair practices that would otherwise fall outside the remit of the Commission.

The repeal of the P2B Regulation would reduce the powers of national regulators, limiting their ability to intervene and protect business users established in their respective Member States. EU-level enforcement cannot sufficiently cover this enforcement gap. As a result, business users can no longer rely on the intervention of their national enforcement body and would face a significant reduction in the level of protection available to them.

3. Transitory regime

Lastly, it should be noted that a transitional regime is provided for certain P2B provisions. Specifically, the Commission's proposal keeps Articles 2(1)(2)(5), 4, 11 and 15 applicable until 31 December 2032. However, as this regime is limited both in substance and time, and as it does not provide any assurance that the substantive obligations contained in the provisions will remain applicable in any other form after 2032, it alone cannot address the concerns expressed in this document.

Aan de Minister van Economische Zaken

Auteur

[Redacted signature block]

TER BESLISSING
Datum aangemaakt
5 maart 2026

Kenmerk
DGED / 104515482

nota
TER BESLISSING

Naderend Raadscompromis Omnibus AI

Kopie aan

Bijlage(n)
4

Parafenroute

[Redacted signature lines]

Aanleiding

Het Cypriotische voorzitterschap zal waarschijnlijk tijdens de Coreper-II-bespreking van 13 maart aanstaande, het bereikte compromis op de Omnibus AI aan de lidstaten voorleggen en een mandaat vragen voor de onderhandelingen met het Europees Parlement (EP). Conform de informatieafspraken met het parlement wordt u verwacht beide Kamers te informeren over de uitkomst van de onderhandelingen over de Omnibus AI en hoe het kabinet deze uitkomst apprecieert.

Geadviseerd besluit

Instemmen met het verzenden van bijgevoegde (inhoudelijk dezelfde) brieven aan de Eerste en Tweede Kamer.

Kernpunten

- 5 maart jl. heeft het Cypriotische voorzitterschap de derde compromistekst gedeeld over de Omnibus AI. De verwachte Raadspositie zal naar verwachting grotendeels in lijn zijn met deze compromistekst. Eerder zou het voorzitterschap streven naar een Raadscompromis eind maart. Dat lijkt nu 13 maart te worden.
- In de Kamerbrieven informeren we beide Kamers over de belangrijkste punten waarop de verwachte Raadspositie op de Omnibus AI zal verschillen van het voorstel van de Europese Commissie. Daarnaast beschrijft de brief hoe deze veranderingen zich verhouden tot de positie van het kabinet.
- In de brief informeren we de Kamers dat we positief zijn over het onderhandelingsresultaat, maar dat we gezien het parlementaire behandelvoorbehoud dat de Eerste Kamer heeft geplaatst bij de digitale omnibussen Nederland zich van stemmen zal moeten onthouden. De brief aan de Eerste Kamer vraagt de Eerste Kamer of zij gezien de verwachte Raadspositie

bereid is het behandelvoorbehoud voor de Omnibus AI op te heffen zodat het kabinet steun kan uitspreken voor het bereikte Raadscompromis.

- De onderdelen van het oorspronkelijke voorstel waar het kabinet positief over was, zijn in de Raadspositie behouden gebleven. In het BNC-fiche heeft het kabinet aangegeven met name op vier punten in te zetten op verbetering van het voorstel. Op al deze punten is de Raadspositie meer in lijn gebracht met de kabinetsinzet ten opzichte van het oorspronkelijke voorstel:
 - *Verwijderen registratieplicht bepaalde AI-systemen die in hoog-risico context worden gebruikt:* Het kabinet heeft ingezet op behoud van deze registratieplicht omdat deze belangrijk is om effectief toezicht te kunnen houden op AI-systemen die in hoog-risico context worden gebruikt. Er lijkt brede steun in de Raad voor behoud van de registratieplicht.
 - *Bevoegdheid voor het verwerken van bijzondere categorieën van persoonsgegevens voor biasdetectie en -correctie:* Het kabinet heeft ingezet op een proportionele, duidelijk afgebakende bevoegdheid, voorzien van waarborgen die de risico's voldoende inperken. Er lijkt voldoende steun om deze bevoegdheid te limiteren tot verwerkingen die strikt noodzakelijk zijn voor het detecteren, corrigeren en voorkomen van bias die waarschijnlijk de gezondheid en veiligheid van personen aantast, grondrechten schaadt of tot discriminatie leidt.
 - *Uitstel van de inwerkingtreding van de bepalingen voor hoog-risico AI-systemen:* Er lijkt brede steun om in lijn met de kabinetsinzet te werken met vaste data voor inwerkingtreding, in plaats van deze data te koppelen aan een Commissiebesluit. Het kabinet heeft liever dat de inwerkingtreding van de bepalingen voor hoog-risico AI-systemen die in bijlage III van de AI-verordening zijn opgenomen minder lang wordt uitgesteld, maar hier is onvoldoende steun voor in de Raad.
 - *AI-geletterdheid:* Het kabinet steunt de doelstelling om AI-geletterdheid te bevorderen bij personeel dat met AI werkt. Het kabinet heeft erop in gezet deze verplichting te verduidelijken of organisaties te ondersteunen bij het voldoen aan deze verplichting. Er lijkt voldoende steun om aanbevelingen en niet-bindende gezamenlijke doelstellingen vast te stellen voor deze verplichting.
- De brief schetst daarnaast nog het krachtenveld op de Omnibus Digitaal. De onderhandelingen op deze omnibus zijn de onderhandelingen nog minder gevorderd. Op verschillende punten van het voorstel waar het kabinet in het BNC-fiche zorgen heeft geuit, lijkt er steun van verschillende lidstaten. Over specifiek (1) het Europees meldpunt en (2) de Platform-to-Business(P2B)-verordening heeft Nederland recent non-papers verspreid, die de zorgen zoals beschreven in het BNC-fiche adresseren. Daarmee dragen deze non-paper dus de staande Nederlandse positie uit. Deze non-papers worden als bijlage bij de brief meegestuurd aan de Kamers.

Krachtenveld

- Het lijkt waarschijnlijk dat de Raadspositie op de Omnibus AI met brede steun wordt aangenomen.