



Eerste Kamer der Staten-Generaal

aan 5.1.2.e

Kazernestraat 52
2514 CV Den Haag
postbus 20017
2500 EA Den Haag

telefoon 070 312 92 00
fax 070 312 93 90

Bijlage 1 – Relevante artikelen uit de Woo

e-mail postbus@eerstekamer.nl
internet www.eerstekamer.nl

Artikel 1.1

Eenieder heeft recht op toegang tot publieke informatie zonder daartoe een belang te hoeven stellen, behoudens bij deze wet gestelde beperkingen.

Artikel 2.1

In deze wet en de daarop berustende bepalingen wordt verstaan onder:
document: een door een orgaan, persoon of college als bedoeld in artikel 2.2, eerste lid, opgesteld of ontvangen schriftelijk stuk of ander geheel van vastgelegde gegevens dat naar zijn aard verband houdt met de publieke taak van dat orgaan, die persoon of dat college;
milieu-informatie: hetgeen daaronder wordt verstaan in artikel 19.1a van de Wet milieubeheer; Onze Minister: Onze Minister van Binnenlandse Zaken en Koninkrijksrelaties;
publieke informatie: informatie neergelegd in documenten die berusten bij een orgaan, persoon of college als bedoeld in artikel 2.2, eerste lid, of informatie die krachtens artikel 2.3 door een bestuursorgaan kan worden gevorderd.

Artikel 2.5

Bij de toepassing van deze wet wordt uitgegaan van het algemeen belang van openbaarheid van publieke informatie voor de democratische samenleving.

Artikel 4.1

1. Eenieder kan een verzoek om publieke informatie richten tot een bestuursorgaan of een onder verantwoordelijkheid van een bestuursorgaan werkzame instelling, dienst of bedrijf. In het laatste geval beslist het verantwoordelijke bestuursorgaan op het verzoek.
2. Een verzoek kan mondeling of schriftelijk worden ingediend en kan elektronisch worden verzonden op de door het bestuursorgaan aangegeven wijze.
3. De verzoeker behoeft bij zijn verzoek geen belang te stellen.
4. De verzoeker vermeldt bij zijn verzoek de aangelegenheid of het daarop betrekking hebbende document, waarover hij informatie wenst te ontvangen.
5. Indien een verzoek te algemeen geformuleerd is, verzoekt het bestuursorgaan binnen twee weken na ontvangst van het verzoek de verzoeker om het verzoek te preciseren en is het de verzoeker daarbij behulpzaam.
6. Het bestuursorgaan kan besluiten een verzoek niet te behandelen, indien de verzoeker niet meewerkt aan een verzoek tot precisering als bedoeld het vijfde lid. In afwijking van artikel 4:5, vierde lid, van de Algemene wet bestuursrecht wordt het besluit om het verzoek niet te behandelen aan de verzoeker bekendgemaakt binnen twee weken

nadat het verzoek is gepreciseerd of nadat de daarvoor gestelde termijn ongebruikt is verstreken.

7. Een verzoek om informatie wordt ingewilligd met inachtneming van het bepaalde in hoofdstuk 5.

Artikel 4.2a

Indien een voldoende gespecificeerd verzoek zodanig omvangrijk is dat niet binnen de termijn van artikel 4.4, eerste lid, kan worden beslist, treedt het bestuursorgaan voor het einde van die termijn in overleg met de verzoeker over de prioritering van de afhandeling van het verzoek. Het bestuursorgaan verstrekt de gevraagde documenten zo veel mogelijk in de door de verzoeker gewenste volgorde.

Artikel 4.3

1. De beslissing op een verzoek om informatie wordt mondeling of schriftelijk genomen.
2. Het bestuursorgaan besluit in ieder geval schriftelijk op een verzoek om informatie, indien:
 - a. het schriftelijke verzoek geheel of gedeeltelijk wordt afgewezen;
 - b. de verzoeker bij gehele of gedeeltelijke afwijzing van het mondelinge verzoek verzoekt om een schriftelijk besluit;
 - c. de gevraagde informatie slechts wordt verstrekt aan de verzoeker overeenkomstig artikel 5.5, artikel 5.6 of artikel 5.7 en aan de verstrekking voorwaarden worden verbonden; of
 - d. de gevraagde informatie betrekking heeft op of afkomstig is van derden, tenzij deze hebben verklaard aan een schriftelijk besluit geen behoefte te hebben.
3. Bij de afwijzing van een mondeling verzoek, wordt de verzoeker gewezen op de mogelijkheid van een schriftelijk besluit.

Artikel 4.4

1. Het bestuursorgaan beslist op het verzoek om informatie zo spoedig mogelijk, doch uiterlijk binnen vier weken gerekend vanaf de dag na die waarop het verzoek is ontvangen.
2. Het bestuursorgaan kan de beslissing voor ten hoogste twee weken verdagen, indien de omvang of de gecompliceerdheid van de informatie een verlenging rechtvaardigt. Van de verdaging wordt voor de afloop van de eerste termijn schriftelijk gemotiveerd mededeling gedaan aan de verzoeker.
3. Onverminderd artikel 4:15 van de Algemene wet bestuursrecht wordt de termijn voor het geven van een beschikking opgeschort gerekend vanaf de dag na die waarop het bestuursorgaan de verzoeker mededeelt dat toepassing is gegeven aan artikel 4:8 van de Algemene wet bestuursrecht, tot en met de dag waarop door de belanghebbende of belanghebbenden een zienswijze naar voren is gebracht of de daarvoor gestelde termijn ongebruikt is verstreken.
4. Indien de opschorting, bedoeld in het derde lid, eindigt, doet het bestuursorgaan daarvan zo spoedig mogelijk mededeling aan de verzoeker, onder vermelding van de termijn binnen welke de beschikking alsnog moet worden gegeven.
5. Indien het bestuursorgaan heeft besloten informatie te verstrekken, wordt de informatie verstrekt tegelijk met de bekendmaking van het besluit, tenzij naar verwachting een belanghebbende bezwaar daartegen heeft, in welk geval de informatie wordt verstrekt twee weken nadat de beslissing is bekendgemaakt. Indien wordt verzocht om een voorlopige voorziening als bedoeld in artikel 8:81 van de Algemene wet bestuursrecht, wordt de

openbaarmaking opgeschort totdat de voorzieningenrechter uitspraak heeft gedaan of het verzoek is ingetrokken.

6. Indien het bestuursorgaan heeft besloten informatie te verstrekken die rechtstreeks betrekking heeft op een derde of die van een derde afkomstig is, deelt het bestuursorgaan dit besluit gelijktijdig mede aan deze derde.

Artikel 4.5

1. Het bestuursorgaan verstrekt de informatie in de door verzoeker verzochte vorm of, indien dit redelijkerwijs niet gevergd kan worden, met inachtneming van het bepaalde in artikel 2.4, derde lid.
2. Indien de informatie reeds in een voor de verzoeker gemakkelijk toegankelijke vorm voor het publiek beschikbaar is, wijst het bestuursorgaan de verzoeker daarop.

Artikel 5.1

1. Het openbaar maken van informatie ingevolge deze wet blijft achterwege voor zover dit:
 - a. de eenheid van de Kroon in gevaar zou kunnen brengen;
 - b. de veiligheid van de Staat zou kunnen schaden;
 - c. bedrijfs- en fabricagegegevens betreft die door natuurlijke personen of rechtspersonen vertrouwelijk aan de overheid zijn meegedeeld;
 - d. persoonsgegevens betreft als bedoeld in paragraaf 3.1 onderscheidenlijk paragraaf 3.2 van de Uitvoeringswet Algemene verordening gegevensbescherming, tenzij de betrokkene uitdrukkelijk toestemming heeft gegeven voor de openbaarmaking van deze persoonsgegevens of deze persoonsgegevens kennelijk door de betrokkene openbaar zijn gemaakt;
 - e. nummers betreft die dienen ter identificatie van personen die bij wet of algemene maatregel van bestuur zijn voorgeschreven als bedoeld in artikel 46 van de Uitvoeringswet Algemene verordening gegevensbescherming, tenzij de verstrekking kennelijk geen inbreuk op de levenssfeer maakt.
2. Het openbaar maken van informatie blijft eveneens achterwege voor zover het belang daarvan niet opweegt tegen de volgende belangen:
 - a. de betrekkingen van Nederland met andere landen en staten en met internationale organisaties;
 - b. de economische of financiële belangen van de Staat, andere publiekrechtelijke lichamen of bestuursorganen, in geval van milieu-informatie slechts voor zover de informatie betrekking heeft op handelingen met een vertrouwelijk karakter;
 - c. de opsporing en vervolging van strafbare feiten;
 - d. de inspectie, controle en toezicht door bestuursorganen;
 - e. de eerbiediging van de persoonlijke levenssfeer;
 - f. de bescherming van andere dan in het eerste lid, onderdeel c, genoemde concurrentiegevoelige bedrijfs- en fabricagegegevens;
 - g. de bescherming van het milieu waarop deze informatie betrekking heeft;
 - h. de beveiliging van personen en bedrijven en het voorkomen van sabotage;
 - i. het goed functioneren van de Staat, andere publiekrechtelijke lichamen of bestuursorganen.
3. Indien een verzoek tot openbaarmaking op een van de in het tweede lid genoemde gronden wordt afgewezen, bevat het besluit hiervoor een uitdrukkelijke motivering.

4. Openbaarmaking kan tijdelijk achterwege blijven, indien het belang van de geadresseerde van de informatie om als eerste kennis te nemen van de informatie dit kennelijk vereist. Het bestuursorgaan doet mededeling aan de verzoeker van de termijn waarbinnen de openbaarmaking alsnog zal geschieden.
5. In uitzonderlijke gevallen kan openbaarmaking van andere informatie dan milieuinformatie voorts achterwege blijven indien openbaarmaking onevenredige benadeling toebrengt aan een ander belang dan genoemd in het eerste of tweede lid en het algemeen belang van openbaarheid niet tegen deze benadeling opweegt. Het bestuursorgaan baseert een beslissing tot achterwege laten van de openbaarmaking van enige informatie op deze grond ten aanzien van dezelfde informatie niet tevens op een van de in het eerste of tweede lid genoemde gronden.
6. Het openbaar maken van informatie blijft in afwijking van het eerste lid, onderdeel c, in geval van milieu-informatie eveneens achterwege voor zover daardoor het in het eerste lid, onderdeel c, genoemde belang ernstig geschaad wordt en het algemeen belang van openbaarheid van informatie niet opweegt tegen deze schade.
7. Het eerste en tweede lid zijn niet van toepassing op milieu-informatie die betrekking heeft op emissies in het milieu.

Artikel 5.2

1. In geval van een verzoek om informatie uit documenten, opgesteld ten behoeve van intern beraad, wordt geen informatie verstrekt over daarin opgenomen persoonlijke beleidsopvattingen. Onder persoonlijke beleidsopvattingen worden verstaan ambtelijke adviezen, visies, standpunten en overwegingen ten behoeve van intern beraad, niet zijnde feiten, prognoses, beleidsalternatieven, de gevolgen van een bepaald beleidsalternatief of andere onderdelen met een overwegend objectief karakter.
2. Het bestuursorgaan kan over persoonlijke beleidsopvattingen met het oog op een goede en democratische bestuursvoering informatie verstrekken in niet tot personen herleidbare vorm. Indien degene die deze opvattingen heeft geuit of zich erachter heeft gesteld, daarmee heeft ingestemd, kan de informatie in tot personen herleidbare vorm worden verstrekt.
3. Onverminderd het eerste en tweede lid wordt uit documenten opgesteld ten behoeve van formele bestuurlijke besluitvorming door een minister, een commissaris van de Koning, Gedeputeerde Staten, een gedeputeerde, het college van burgemeester en wethouders, een burgemeester en een wethouder, informatie verstrekt over persoonlijke beleidsopvattingen in niet tot personen herleidbare vorm, tenzij het kunnen voeren van intern beraad onevenredig wordt geschaad.
4. In afwijking van het eerste lid wordt bij milieu-informatie het belang van de bescherming van de persoonlijke beleidsopvattingen afgewogen tegen het belang van openbaarmaking. Informatie over persoonlijke beleidsopvattingen kan worden verstrekt in niet tot personen herleidbare vorm. Indien degene die deze opvattingen heeft geuit of zich erachter heeft gesteld, daarmee heeft ingestemd, kan de informatie in tot personen herleidbare vorm worden verstrekt.

Artikel 5.3

Bij een verzoek om informatie die ouder is dan vijf jaar motiveert het bestuursorgaan bij een weigering van die informatie waarom de in artikel 5.1, tweede of vijfde lid, of artikel 5.2 bedoelde belangen ondanks het tijdsverloop zwaarder wegen dan het algemeen belang van openbaarheid.

Artikel 5.5

1. Onverminderd het elders bij wet bepaalde, verstrekt een bestuursorgaan iedere natuurlijke of rechtspersoon op diens verzoek de op de verzoeker betrekking hebbende in documenten neergelegde informatie, tenzij een in artikel 5.1, eerste lid, onderdelen a, b en c, alsmede d en e, voor zover betrekking hebbend op derden, genoemd belang aan de orde is of een in artikel 5.1, tweede of vijfde lid, of artikel 5.2 genoemd belang zwaarder weegt dan het belang van de verzoeker bij toegang tot op hem betrekking hebbende informatie. De verzoeker vermeldt bij zijn verzoek de aangelegenheid of het daarop betrekking hebbende document, waarover hij informatie wenst te ontvangen.
2. Het eerste lid is van overeenkomstige toepassing op een verzoek met betrekking tot gegevens ten aanzien van een overleden echtgenoot, geregistreerd partner, kind of ouder van de verzoeker, tenzij een schriftelijke wilsverklaring van de overledene aan de verstrekking in de weg staat.
3. Het bestuursorgaan draagt zorg voor een deugdelijke vaststelling van de identiteit van de verzoeker.
4. Het bestuursorgaan kan aan de verstrekking voorwaarden verbinden ter bescherming van een van de belangen, genoemd in de artikelen 5.1 en 5.2, tenzij de gevraagde informatie met toepassing van de artikelen 5.1 en 5.2 openbaar voor eenieder zou zijn.

Artikel 5.6

1. Het bestuursorgaan kan, in geval informatie ingevolge de artikelen 5.1 en 5.2 niet openbaar gemaakt kan worden, besluiten de informatie uitsluitend aan de verzoeker te verstrekken, indien er klemmende redenen zijn om de verzoeker niettegenstaande de toepasselijke uitzonderingsgrond of -gronden de gevraagde informatie niet te onthouden.
2. Het eerste lid vindt slechts toepassing voor zover dit niet in strijd is met een toepasselijke geheimhoudingsplicht.
3. Het bestuursorgaan kan aan de verstrekking voorwaarden verbinden ter bescherming van een van de belangen, genoemd in de artikelen 5.1 en 5.2.

Artikel 5.7

1. Een bestuursorgaan kan ten behoeve van historisch, statistisch, wetenschappelijk of journalistiek onderzoek toegang bieden tot informatie:
 - a. die ingevolge de artikelen 5.1 en 5.2 niet openbaar gemaakt kan worden; of
 - b. waarvan de vaststelling of deze informatie ingevolge de artikelen 5.1 en 5.2 openbaar gemaakt kan worden een onevenredige inspanning vergt.
2. Het bestuursorgaan kan aan het verlenen van toegang voorwaarden verbinden.
3. De toegang tot informatie overeenkomstig het eerste lid wordt in ieder geval verleend onder de voorwaarde dat degene aan wie toegang wordt verleend, de verkregen informatie niet verder verspreidt zonder voorafgaand besluit van het bestuursorgaan waarin de informatie met toepassing van de artikelen 5.1 en 5.2 openbaar gemaakt wordt.

#	Bestandsnaam	Weigeringsgrond	Toelichting
1	RE Notitie - Digital Omnibus-wetgeving van de Europese Commissie.pdf	5.1.2.e, 5.2,1	
2	Bericht op website over rapporteurs.pdf	5.1.2.e	
3	RE Goed om te weten, save-the-date.pdf	5.1.2.e, 5.2,1	
4	FW MinvEZK EK Naderend Raadscompromis Omnibus AI.pdf	5.1.2.e, 5.2,1	
5	104512038 EK Beslisnota Naderend Raadscompromis Omnibus AI.pdf		
6	104512038 Bijlage 1 Non-paper Omnibus SEP.pdf		
7	104512038 Bijlage 2 P2B non-paper regarding Omnibus VII.pdf		
8	104512038 Brief EK Naderend Raadscompromis Omnibus AI.docx		
9	mandaatstekst als resultaat van Antici-vergadering van gisteren.pdf	5.1.2.e, 5.2,1	
10	MinvEZK Beantwoording EK-vragen Omnibus AI, Omnibus Digitaal en Data Unie Strategie.pdf	5.1.2.e, 5.2,1	
11	104349249 Beantwoording EK-vragen Omnibus AI, Omnibus Digitaal en Data Unie Strategie.docx		
12	104349249 Beslisnota bij Beantwoording Eerste Kamervragen Omnibus AI, Omnibus Digitaal en Data Unie Strategie.pdf		
13	Brief DIGI EZKGG stasEZ inzake Omnibus Digitaal, Omnibus AI en Data Unie Strategie.docx		
14	RE Advies TCGCT over omnibussen AI en Digitaal .pdf	5.1.2.e, 5.2,1	
15	RE French Senate PPRE avis motivé CSA2 et PPRE omnibus numérique.pdf	5.1.2.e, 5.2,1	
16	Re Gesprekspunten overleg rapporteurs.pdf	5.1,2,E, 5.1.2.e, 5.2,1	
17	antwoordbrief Europese Commissie op commissievragen omnibussen.pdf	5.1.2.e, 5.2,1	
18	C_2026_3661_1_NL_ACT_part1_v3.docx	5.1.2.e, 5.2,1	
19	20260619 VSO DIGI EZ KGG 36890 ek-W (bijlage).pdf	5.1.2.e, 5.2,1	
20	FW Kamerbrief aan de Eerste Kamer inzake beantwoording schriftelijke vragen inzake de inzet van de omnibusprocedure.pdf	5.1.2.e	
21	Beantwoording schriftelijke vragen inzake de inzet van de omnibusprocedure.docx		
22	Beslisnota bi Beantwoording schriftelijke vragen inzake de inzet van de omnibusprocedure.pdf		
23	1. korte notitie - Natali Helberger.pdf		
24	uitnodiging voor een gesprek met de rapporteurs over de (impact van de) omnibus AI & omnibus digitaal, gericht op samenhang met andere regelgeving en de feitelijke werking van het juridisch kader.docx	5.1.2.e	
25	uitnodiging voor een gesprek met de rapporteurs over de (impact van de) omnibus AI & omnibus digitaal, met een focus van de impact op grondrechten.docx	5.1.2.e	

26	uitnodiging voor een gesprek 'regeldruk, uitvoerbaarheid en impact op concurrentiekracht' met de rapporteurs over de omnibus AI & omnibus digitaal.docx	5.1.2.e	
27	uitnodiging voor een gesprek met de rapporteurs over de (impact van de) omnibus AI & omnibus digitaal, met een focus van de impact op grondrechten.docx	5.1.2.e	
28	uitnodiging voor een gesprek 'regeldruk, uitvoerbaarheid en impact op concurrentiekracht' met de rapporteurs over de omnibus AI & omnibus digitaal.docx	5.1.2.e	
29	1. white paper - Laura Drechsler.pdf		
30	105571251 Beslisnota consultaties en Kamerbrief uitvoeringswet AI-verordening.pdf		
31	105571251 Kamerbrief Inrichting toezicht op de naleving van de AI-verordening.docx	5.1.2.e	
32	20260211 - BusinessEurope Position Paper - Making the General Data Protection Regulation more effective.pdf	5.1.2.e	
33	Adviescollege toetsing regeldruk.pdf		
34	CWO-CPR 26-09 Input VNO-NCW and MKB-Nederland Digital Fitness Check.pdf	5.2,1	
35	Final BusinessEurope Statement - Digital Omnibus (GDPR).pdf		
36	Joint Statement B9+ Digital Omnibus.pdf		
37	Notitie EK-CRM Digitale Omnibus Pakket 29 april.pdf		
38	position paper - AP.pdf		
39	position paper - Bits of Freedom & Stichting Databescherming.pdf		
40	Position Paper VNO-NCW en MKB-Nederland Digital Omnibus 11 mei 2026 def.pdf	5.1.2.e	
41	VNO-NCW MKB-Nederland Positie Paper Digital Omnibus (on AI) 20260213.pdf	5.2,1	
n.v.t.	FW Digitale technische briefing over artificiële intelligentie.pdf	5.2 lid 1	Niet openbaar
n.v.t.	Technische briefing Artificial intelligence_besloten bijeenkomst.pptx	5.1 lid 1	Niet openbaar
n.v.t.	FW notitie voor de commissie EUZA.pdf	5.2 lid 1	Niet openbaar
n.v.t.	Notitie EUZA - Notitie omnibusprocedure en impact assessments - eindversie (12062026.opmID).docx	5.2 lid 1	Niet openbaar
n.v.t.	Brief over naderend raadscompromis inclusief antwoorden op vragen non-paper.pdf	5.2 lid 1	Niet openbaar
n.v.t.	uitnodiging nationale toezichthouders voor een gesprek met de rapporteurs over de omnibus AI & omnibus digitaal.docx	5.2 lid 1	Niet openbaar

From: "5.1.2.e"
Sent: Fri, 21 Nov 2025 14:17:58 +0100
To: "Cees van de Sanden" <cees.vandesanden@eerstekamer.nl>
Cc: "Gala Veldhoen" <gala.veldhoen@eerstekamer.nl>
Subject: RE: Notitie - Digital Omnibus-wetgeving van de Europese Commissie

Beste Cees,

5.1.2.e

5.1.2.e

5.1.2.e

5.1.2.e

5.1.2.e

5.2,1

In het bij het agendapunt gevoegde rapport van de onderzoeksafdeling van het Europees Parlement trof ik onderstaande passage (p.37).

“Moreover, the executability of data subject rights is uncertain once personal data has been absorbed into AI systems. Access, rectification, erasure and objection remain guaranteed under Articles 15-22 of the GDPR, yet neither framework provides workable methods to action these rights when data has been dispersed into model weights, embeddings or captured in logs retained for AI Act traceability. User prompts may themselves contain personal data, but once stored for monitoring, they cannot be selectively erased without compromising system integrity. Controllers remain bound to honour requests they cannot technically fulfil, while providers are required to preserve evidence for conformity. The result is not a legislative void, but an implementation problem. Rights exist on paper, but their operational delivery is practically infeasible.”

[interplay between the AI Act en the EU digital legislative framework](#)

Met vriendelijke groet,

5.1.2.e

Plaatsvervangend griffier

(griffier commissie Digitalisering)

Eerste Kamer der Staten-Generaal
Kazernestraat 52 (kamer 137)

2514 CV Den Haag

Postbus 20017
2500 EA Den Haag

M 5.1.2.e
E 5.1.2.e @eerstekamer.nl
I www.eerstekamer.nl

De Eerste Kamer wil graag weten hoe je onze website ervaart.

Vul de korte enquête in op www.eerstekamer.nl!

Van: Cees van de Sanden <cees.vandesanden@eerstekamer.nl>

Verzonden: donderdag 20 november 2025 14:02

Aan: 5.1.2.e <5.1.2.e@eerstekamer.nl>; Gala Veldhoen <gala.veldhoen@eerstekamer.nl>

Onderwerp: Notitie - Digital Omnibus-wetgeving van de Europese Commissie

5.2.1 5.1.2.e

5.2.1

5.2.1

Dank en groet,

Fractie Van de Sanden

Cees van de Sanden

Onafhankelijk liberaal senator

From: "5.1.2.e"
Sent: Tue, 3 Mar 2026 16:11:47 +0100
To: "Mary Fiers" <mary.fiers@eerstekamer.nl>; "Cees van de Sanden" <cees.vandesanden@eerstekamer.nl>
Bcc: "5.1.2.e" <5.1.2.e@eerstekamer.nl>
Subject: Bericht op website over rapporteurs

Beste Mary en Cees,

Ter informatie.

Met vriendelijke groet,

5.1.2.E

Plaatsvervangend griffier

(griffier commissie Digitalisering)

Eerste Kamer *der Staten-Generaal*

Kazernestraat 52 (kamer 137)

2514 CV Den Haag

Postbus 20017

2500 EA Den Haag

M 5.1.2.e

E 5.1.2.e [@eerstekamer.nl](mailto:5.1.2.e@eerstekamer.nl)

I www.eerstekamer.nl

Van: 5.1.2.e <5.1.2.e@eerstekamer.nl>

Verzonden: dinsdag 3 maart 2026 15:40

Aan: 5.1.2.e <5.1.2.e@eerstekamer.nl>

Onderwerp: RE: Berichtje rapporteurs

Hoi 5.1.2.e

Ter info. Het nieuwsbericht staat online op de website en is gedeeld op X en Bluesky: [Eerste Kamer benoemt rapporteurs EU-wetgeving digitalisering en AI - Eerste Kamer der Staten-Generaal](#)

We maken ook nog een berichtje voor LinkedIn.

Groeten,

5.1.2.e

Persvoorlichter / woordvoerder

Eerste Kamer *der Staten-Generaal*

Bezoekadres

Kazernestraat 52
2514 CV Den Haag

Postadres

Postbus 20017
2500 EA Den Haag

M 5.1.2.e
E 5.1.2.e [@eerstekamer.nl](mailto:5.1.2.e@eerstekamer.nl)
I www.eerstekamer.nl



From: "Mary Fiers"
Sent: Fri, 6 Mar 2026 23:46:04 +0100
To: "5.1.2.e" <5.1.2.e@eerstekamer.nl>; "Cees van de Sanden" <cees.vandesanden@eerstekamer.nl>
Cc: "5.1.2.e" <5.1.2.e@eerstekamer.nl>
Subject: RE: Goed om te weten; save-the-date

Ha 5.2,1

5.2,1

5.2,1

5.2,1

5.2,1

Hartelijke groeten,

Mary Fiers

Senator

Woordvoerder Binnenlandse Zaken en digitalisering



Van: 5.1.2.e <5.1.2.e@eerstekamer.nl>

Verzonden: vrijdag 27 februari 2026 11:26

Aan: Cees van de Sanden <cees.vandesanden@eerstekamer.nl>; Mary Fiers <mary.fiers@eerstekamer.nl>

CC: 5.1.2.e <5.1.2.e@eerstekamer.nl>

Onderwerp: Goed om te weten; save-the-date

5.2,1

5.2,1

5.2,1 5.1.2.e

In bijgevoegd bericht op de website van Corporate Europe Observatory wordt in een open brief aandacht gevraagd voor het feit dat Aura Salla voorheen jarenlang lobbyist is geweest voor Meta.

[Watchdog organisations issue call to withdraw Aura Salla's appointment as Digital Omnibus rapporteur | Corporate Europe Observatory](#)

“In her [declaration of awareness for her role as Rapporteur](#) of the Digital Omnibus, she failed to indicate her previous work at Meta as a potential conflict of interest as required by Article 3 of the Code of Conduct for Members of the European parliament.”

5.1.2.e

5.1.2.e

5.1.2.e

5.2.1

Met vriendelijke groet,

5.1.2.E

Plaatsvervangend griffier

(griffier commissie Digitalisering)

Eerste Kamer *der Staten-Generaal*
Kazernestraat 52 (kamer 137)

2514 CV Den Haag

Postbus 20017
2500 EA Den Haag

M 5.1.2.e

E 5.1.2.e @eerstekamer.nl

I www.eerstekamer.nl

From: "5.1.2.e"
Sent: Sun, 8 Mar 2026 17:05:51 +0100
To: "Cees van de Sanden" <cees.vandesanden@eerstekamer.nl>; "Mary Fiers" <mary.fiers@eerstekamer.nl>
Cc: "Gala Veldhoen" <gala.veldhoen@eerstekamer.nl>
Subject: FW: MinvEZK: EK Naderend Raadscompromis Omnibus AI
Attachments: 104512038 EK Beslisnota Naderend Raadscompromis Omnibus AI.pdf, 104512038 Bijlage 1 Non-paper Omnibus SEP.pdf, 104512038 Bijlage 2 P2B non-paper regarding Omnibus VII.pdf, 104512038 Brief EK Naderend Raadscompromis Omnibus AI.docx

5.1.2.e en 5.1.2.e

De bedoelde brief van de staatssecretaris is ontvangen.

5.2.1
 5.2.1
 5.2.1
 5.2.1
 5.2.1

Ik zal deze morgenochtend verwerken in het convocaat van de combi-vergadering.

Met vriendelijke groet,

5.1.2.E

Plaatsvervangend griffier

(griffier commissie Digitalisering)

Eerste Kamer *der Staten-Generaal*
 Kazernestraat 52 (kamer 137)

2514 CV Den Haag

Postbus 20017
 2500 EA Den Haag

M 5.1.2.e
E 5.1.2.e @eerstekamer.nl
I www.eerstekamer.nl

Van: 5.1.2.e <5.1.2.e@eerstekamer.nl>

Verzonden: zaterdag 7 maart 2026 13:28

Aan: 5.1.2.e <5.1.2.e@eerstekamer.nl>; 5.1.2.e <5.1.2.e@eerstekamer.nl>; 5.1.2.e <5.1.2.e@eerstekamer.nl>

Onderwerp: Fw: MinvEZK: EK Naderend Raadscompromis Omnibus AI

En de brief aan ons

Aan de Minister van Economische Zaken

Directoraat-generaal
Economie en Digitalisering

Auteur
[Redacted]
[Redacted]
[Redacted]

TER BESLISSING
Datum aangemaakt
5 maart 2026

Kenmerk
DGED / 104515482

Kopie aan
[Redacted]

Bijlage(n)
4

nota
TER BESLISSING

Naderend Raadscompromis Omnibus AI

Parafenroute		
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]		[Redacted]
[Redacted]		[Redacted]

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.

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.

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

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 het mondeling overleg met de Eerste Kamer op 17 maart in 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. Ik zal uw Kamer in de week van 9 maart de beantwoording van uw schriftelijke vragen over de omnibussen en de bijbehorende BNC-fiches toesturen.

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 uw Kamer heeft geplaatst bij de Omnibus AI en Omnibus Digitaal zal het kabinet zich 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 wil ik uw Kamer vragen of

**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 / 104512038

Uw kenmerk
179856

Bijlage(n)
2

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

zij bereid is het behandelvoorbehoud op de Omnibus AI op te heffen zodat het kabinet zich positief kan uitspreken over de bereikte Raadscompromis. Indien uw Kamer hier niet toe bereid is 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 geldende 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

From: "5.1.2.e"
Sent: Tue, 10 Mar 2026 14:38:27 +0100
To: "Cees van de Sanden" <cees.vandesanden@eerstekamer.nl>; "Mary Fiers" <mary.fiers@eerstekamer.nl>
Subject: 5.2.1 5.2.1
Attachments: st06969-re01.en26.pdf

Hoi Cees en Mary,

5.2.1

Met vriendelijke groet,

5.1,2,E

Plaatsvervangend griffier

(griffier commissie Digitalisering)

Eerste Kamer *der Staten-Generaal*
Kazernestraat 52 (kamer 137)

2514 CV Den Haag

Postbus 20017
2500 EA Den Haag

M 5.1.2.e
E 5.1.2.e [@eerstekamer.nl](mailto:5.1.2.e@eerstekamer.nl)
I www.eerstekamer.nl

From: "5.1.2.e"
Sent: Fri, 13 Mar 2026 11:12:39 +0100
To: "5.1.2.e" <5.1.2.e@eerstekamer.nl>; "5.1.2.e" <5.1.2.e@eerstekamer.nl>
Subject: MinvEZK: Beantwoording EK-vragen Omnibus AI, Omnibus Digitaal en Data Unie Strategie
Attachments: 104349249 Beantwoording EK-vragen Omnibus AI, Omnibus Digitaal en Data Unie Strategie.docx, 104349249 Beslisnota bij Beantwoording Eerste Kamervragen Omnibus AI, Omnibus Digitaal en Data Unie Strategie.pdf, Brief DIGI EZKGG stasEZ inzake Omnibus Digitaal, Omnibus AI en Data Unie Strategie.docx

Geachte leden van de commissies DIGI en EZ/KGG,

Bijgevoegd treft u de antwoorden aan op de vragen die vanuit uw commissies zijn gesteld over de Omnibus AI, de Omnibus Digitaal en de Data Unie Strategie. De uitgaande brief van de commissies is tevens bijgesloten.

5.2.1

5.2.1

Met vriendelijke groet,

5.1.2.E

Plaatsvervangend griffier

(griffier commissie Digitalisering)

Eerste Kamer *der Staten-Generaal*
Kazernestraat 52 (kamer 137)

2514 CV Den Haag

Postbus 20017
2500 EA Den Haag

M 5.1.2.e

E 5.1.2.e [@eerstekamer.nl](mailto:5.1.2.e@eerstekamer.nl)

I www.eerstekamer.nl

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

**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

Datum 13 maart 2026
Betreft Beantwoording vragen Omnibus AI, Omnibus Digitaal en Data Unie
Strategie

Ons kenmerk
DGED / 104349249

Uw kenmerk
179856

Geachte Voorzitter,

Hierbij zend ik u, mede namens de minister van Binnenlandse Zaken en Koninkrijksrelaties, de minister van Justitie en Veiligheid en de staatssecretaris van Justitie en Veiligheid, de antwoorden op de vragen van de leden van de fracties van GroenLinks-PvdA, BBB, D66, mede namens de leden van de fractie van de PvdD, PVV, Volt en fractie-Van de Sanden naar aanleiding van de voorstellen voor de Omnibus Digitaal (COM(2025)837), Omnibus AI (COM(2025)836) en de Data Unie Strategie (COM(2025)835), evenals de bijbehorende BNC-fiches (179856, ingezonden 24 februari 2026).

In lijn met het door uw Kamer geplaatste parlementair behandelvoorbehoud maakt het kabinet tot het mondeling overleg dat 17 maart met uw Kamer zal plaatsvinden in 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. In dat kader heeft het kabinet ook met gelijkgestemde lidstaten non-papers verspreid die de zorgen over het intrekken van de P2B-verordening en het op te richten Europees meldpunt adresseren.

Ik stel voor met uw Kamer dezelfde informatie-afspraken te maken als het kabinet met de Tweede Kamer heeft gemaakt. Dat zou inhouden dat ik uw Kamer regulier update over de onderhandelingen via de geannoteerde agenda voor de Telecomraad. Indien nodig zal ik uw Kamer aanvullend daarop nog per brief informeren wanneer er bijvoorbeeld sprake is van een naderend akkoord. Ik streef ernaar uw Kamer ondanks de hoge snelheid van de onderhandelingen zo goed mogelijk over de voortgang van de onderhandelingen te informeren. Daarbij ben ik wel gebonden aan de informatie-afspraken binnen de Raad en de vertrouwelijkheid van onderhandelingsstukken.

179856

Vragen van de leden van de fractie van GroenLinks-PvdA

1

Algemene vragen

De leden van de fractie van GroenLinks-PvdA merken op dat er geen integrale impact assessment is gemaakt van Omnibus Digitaal, de Omnibus AI en de Data Unie Strategie. Dat vinden deze leden zeer zorgelijk. In het BNC-fiche lezen deze leden dat ook de regering hier zorgen over heeft. De leden merken op dat een impact assessment vereist is voor Europese voorstellen die mogelijk significante economische, ecologische of sociale gevolgen hebben. Dit geldt voor zowel wetgevingsvoorstellen (richtlijnen/verordeningen) als belangrijke niet-wetgevingsinitiatieven (zoals mededelingen of actieplannen). Een impact assessment is onderdeel van de agenda "Better Regulation" (betere regelgeving) van de Europese Commissie.

Deelt u de conclusie van deze leden dat een integrale impact assessment een verplicht onderdeel is? Zo nee, waarom niet? Zo ja, wat betekent deze verplichting voor de kabinetsinzet? Is dit een harde voorwaarde om te kunnen starten met de onderhandelingen en/of in te kunnen stemmen met de voorstellen? Deze leden ontvangen graag een toelichting.

Antwoord

Voor de omnibussen presenteert de Europese Commissie (hierna: Commissie) in het algemeen geen impact assessments. De Commissie geeft als reden dat het gaat om urgente aanpassingen van politiek belang, die te veel vertraging zouden oplopen als er een volledig impact assessment moet worden uitgevoerd. De analyse en onderbouwing van de voorstellen wordt middels een Staff Working Document (SWD)¹ gedeeld.

Het SWD biedt volgens de Commissie voldoende basis om te onderhandelen over de voorstellen die zich in lijn met de kabinetsinzet focussen op versimpelen, verduidelijken en stroomlijnen. Voor sommige onderdelen van de voorstellen die verdergaan dan het versimpelen, verduidelijken en stroomlijnen van wetgeving, maakt het ontbreken van een impact assessment het moeilijk voor het kabinet om de effecten te beoordelen.

Het kabinet heeft de Commissie verzocht een uitgebreidere analyse van de impact van deze voorstellen te presenteren. Ook brengt het kabinet zelf de gevolgen van de voorstellen verder in kaart. Daarmee zet het kabinet erop in de voorstellen die verdergaan dan versimpeling te behandelen op een wijze die recht doet aan de potentiële impact en de zorgpunten. Een formeel impact assessment is niet de enige manier om deze inzet te bewerkstelligen. Het kabinet heeft daarnaast aangegeven dat het advies van de Europees Toezichthouder voor gegevensbescherming (EDPS) en het Europees Comité voor gegevensbescherming

¹ [Digital Omnibus Regulation Proposal | Shaping Europe's digital future](#)

(EDPB), dat 10 februari is vastgesteld, moet worden betrokken bij de bespreking van dit voorstel.² Het advies van de EDPB en EDPS is op voorspraak van Nederland gepresenteerd in de AGS. Ook brengt het kabinet zelf de gevolgen van de voorstellen verder in kaart. Daarmee zet het kabinet erop in de voorstellen die verdergaan dan versimpeling te behandelen op een wijze die recht doet aan de potentiële impact en de zorgpunten.

2

De leden van de fractie van GroenLinks-PvdA merken op dat als de Europese Commissie bij een voorstel voor een verordening geen impact assessment maakt, lidstaten en andere actoren verschillende politieke en juridische mogelijkheden hebben om de Europese Commissie hiertoe aan te sporen. Verordeningen zijn rechtstreeks van toepassing in lidstaten en hebben dus directe werking, waardoor actie tijdens het wetgevingsproces cruciaal is.

Welke mogelijkheden ziet u om tijdig een integrale impact assessment beschikbaar te krijgen? Deze leden ontvangen hier graag een volledige opsomming van.

Antwoord

Het kabinet heeft in de onderhandelingen herhaaldelijk om een impact assessment gevraagd en ook tijdens de Telecomraad van 5 december 2025 hiertoe opgeroepen. Het kabinet ziet weinig kans dat er alsnog aan deze oproep gehoor wordt gegeven aangezien de Commissie in het algemeen geen impact assessments voor omnibussen uitvoert, ook niet na oproepen van lidstaten dit alsnog te doen. Bovendien lijkt er onvoldoende steun om de Commissie hiertoe te blijven oproepen.

Zoals aangegeven in de beantwoording van vraag 1 zet het kabinet erop in de voorstellen die verdergaan dan versimpeling te behandelen op een wijze die recht doet aan de potentiële impact en de zorgpunten. Een formeel impact assessment is niet de enige manier om deze inzet te bewerkstelligen. Het kabinet heeft de Commissie verzocht een uitgebreidere analyse van de impact van deze voorstellen te presenteren. Ook brengt het kabinet zelf de gevolgen van de voorstellen verder in kaart en hecht het zeer aan het gezamenlijke advies van de EDPB en EDPS.

3

Welke mogelijkheden bent u voornemens om in te zetten?

Antwoord

Het kabinet spant zich er met name voor in om voldoende informatie te verkrijgen om de voorstellen goed te kunnen beoordelen. Een formeel impact assessment is niet de enige manier om deze inzet te bewerkstelligen. Het kabinet heeft in de onderhandelingen en via bilaterale gesprekken over verschillende onderdelen van de omnibussen opheldering gevraagd. Ook brengt het kabinet zelf de gevolgen

² [Digitale omnibus: EDPB en EDPS ondersteunen vereenvoudiging en concurrentievermogen en maken zich grote zorgen | European Data Protection Board](#)

van de voorstellen verder in kaart en heeft het kabinet verzocht de adviezen van de EDPS en de EDPB bij de onderhandelingen te betrekken. Dat laatste gebeurt inmiddels.

4

Ziet u kansen om hierbij allianties met andere landen te vormen? Deze leden ontvangen graag een toelichting.

Antwoord

Niet voor een specifieke oproep voor een impact assessment. De oproep voor meer informatie en onderbouwing bij de voorstellen wordt wel breder gedeeld en wordt deels gefaciliteerd binnen de onderhandelingen.

5

Ziet u kansen om hierbij een beroep te doen op het Interinstitutioneel Akkoord Beter Wetgeven? Deze leden ontvangen graag een toelichting.

Antwoord

Het kabinet heeft de Commissie verzocht een uitgebreidere analyse van de impact van deze voorstellen te presenteren. Ook brengt het kabinet zelf de gevolgen van de voorstellen verder in kaart. Daarmee zet het kabinet erop in de voorstellen die verdergaan dan versimpeling te behandelen op een wijze die recht doet aan de potentiële impact en de zorgpunten.

6

Hoe verhouden de Data Unie strategie, de Omnibus Digitaal en de Omnibus AI zich tot de doelstellingen van de Nationale Digitalisering Strategie? Deze leden ontvangen graag een toelichting.

Antwoord

Conform de interventies van de NDS zet het kabinet zich in voor de implementatie van digitale wetgeving en het wegnemen van juridische knelpunten. Overheidsinstanties en medeoverheden staan onder een grote druk om verschillende soort Europese wetgeving op het digitale terrein in samenhang te implementeren en uit te voeren. Het kabinet staat dus vanuit de NDS positief tegenover de Omnibus Digitaal en de Omnibus AI in hun doelstellingen om wet- en regelgeving te versimpelen. Daarnaast onderstreept de Data Unie Strategie het belang van data voor AI en zet het in op het vergroten van interoperabiliteit waarbij privacy en Europese waarden beschermd blijven. Dit sluit goed aan op de doelstellingen van de NDS en in het bijzonder de prioriteit data, waar het wegnemen van knelpunten in gegevensdeling en het federatief datastelsel belangrijke elementen zijn.

De doelstelling van de omnibussen sluiten daarnaast goed aan bij pijler 3 van de Strategie Digitale Economie³. Het verduidelijken, versimpelen en versterken van

³ Kamerstukken II 2022/2023, 26643, nr. 941

de samenhang van digitale wetgeving draagt bij aan het creëren van de juiste randvoorwaarden voor goedwerkende digitale markten en diensten.

7

Welke wet- en regelgeving wordt door deze aanpassingen geraakt, direct dan wel indirect? Worden de Wet politiegegevens en de Wet justitiële en strafvorderlijke gegevens bijvoorbeeld geraakt?

Antwoord

De Omnibus AI wijzigt de AI-verordening en bevat enkele technische wijzigingen aan de verordening inzake gemeenschappelijke regels op het gebied van burgerluchtvaart en tot oprichting van een Agentschap van de Europese Unie voor de veiligheid van de luchtvaart. Op dit moment wordt gewerkt aan een wetsvoorstel ter uitvoering van de AI-verordening. Dit wetsvoorstel dient na inwerkingtreding van de Omnibus AI mogelijk te worden gewijzigd.

De wetgeving die door de Omnibus Digitaal wordt gewijzigd, onder andere de Dataverordening, Datagovernanceverordening (DGA) en Platform-to-Business(P2B)-verordening, zijn wel al uitgevoerd in Nederland. Afhankelijk van de definitieve inhoud van de Omnibus Digitaal zullen de nationale uitvoeringswetten van deze verordeningen moeten worden aangepast. De voorgestelde wijzigingen uit de Omnibus Digitaal betekenen dat de Uitvoeringswet datagovernanceverordening en de Wet hergebruik van overheidsinformatie (Who) waarschijnlijk moeten worden ingetrokken en dat de Uitvoeringswet dataverordening moet worden gewijzigd, ten dele om de inhoud van de (voormalige) Uitvoeringswet datagovernanceverordening en Who daarin op te nemen. De introductie van hoofdstuk VIIc van de Omnibus Digitaal zal tot het opstellen of het aanpassen van de nationale uitvoeringswetten leiden. Verder wordt door de Omnibus Digitaal de P2B-verordening gefaseerd ingetrokken. Dit heeft tot gevolg dat de Wet publiek toezicht en handhaving verordening bevordering billijkheid en transparantie voor zakelijke gebruikers van onlinetussenhandelsdiensten moet worden aangepast en op termijn moet worden ingetrokken. In Boek 3 van het Burgerlijk Wetboek en het Wetboek van Burgerlijke Rechtsvordering zijn bepalingen opgenomen ter uitvoering van de regels uit de P2B verordening inzake collectieve acties. Deze bepalingen moeten ook worden geschrapt.

De voorgestelde wijzigingen van het Europese gegevensbeschermingsrecht zien in eerste instantie alleen op AVG zelf en niet op de Rechtshandavingsrichtlijn,⁴ waarvan de Wet politiegegevens (Wpg) en de Wet justitiële en strafvorderlijke gegevens (Wjsg) de implementatie vormen. Op het moment dat er wijzigingen plaatsvinden in kernbepalingen uit de AVG die ook voorkomen in de richtlijn, zoals de definitie van persoonsgegevens, zal er vanwege de consistentie en coherentie

⁴ Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad.

een wijziging nodig kunnen zijn van de Rechtshandavingsrichtlijn. Het voorstel bepaalt daarom dat na vaststelling van de Digitale omnibus “de nodige aanpassingen” moeten plaatsvinden aan de Richtlijn Gegevensbescherming bij Rechtshandhaving (RGR).⁵ Dat vergt dan een voorstel van de Commissie om deze richtlijn aan te passen. Om juridische redenen kan dat niet in de Digitale omnibus zelf. Afhankelijk van de definitieve tekst van de Digitale omnibus en van het voorstel is daarom niet ondenkbaar dat er impact zal zijn op de Wpg en Wjsg. Er lijkt echter voldoende steun in de Raad om de wijziging van de definitie van persoonsgegevens terug te draaien.

In het BNC-fiche⁶ is ten aanzien van de wijzigingen van de AVG aangegeven dat deze voorstellen “mogelijk” dient te leiden tot wijziging van Nederlandse regelgeving, en dat dit nader zal worden onderzocht. Omdat de voorstellen nu echter nog niet definitief zijn, is het moeilijk nu al uitsluitsel te geven over welke aanpassing uiteindelijk nodig zal zijn. Niet uit te sluiten valt bijvoorbeeld dat een wetstechnische aanpassing nodig is van artikel 40 van de Uitvoeringswet AVG in verband met de voorgestelde formulering van artikel 22 AVG inzake geautomatiseerde individuele besluitvorming, tenzij de alternatieve formulering van de EDPB en EDPS wordt overgenomen. Verder biedt het voorgestelde artikel 88c de mogelijkheid om in de nationale wetgeving te bepalen dat voor de verwerking van persoonsgegevens in AI-context uitdrukkelijk toestemming vereist is. Indien Nederland hiervan gebruik zou willen maken, vergt dit een wetswijziging. Er zijn vooralsnog geen indicaties voor overige (substantiële) punten waarbij de voorgestelde wijzigingen van de AVG een wetswijziging met zich zouden kunnen brengen. Verder lijkt de wijziging van de e-Privacyrichtlijn een kleine aanpassing van hoofdstuk 11 van de Telecommunicatiewet te vergen.

8

Welke uitvoeringsorganisaties worden geraakt door deze aanpassingen? Deze leden ontvangen graag een toelichting.

Antwoord

De overheidsorganisaties die het meest worden geraakt door deze wijzigingen zijn de organisaties die uitvoering geven aan, of toezicht houden op, de wetten die worden gewijzigd. Dat zijn primair de Autoriteit Persoonsgegevens (AP) en de Autoriteit Consument en Markt (ACM). Voor wat betreft de opname van de Open Data Richtlijn wordt Logius, als nationaal dataportaal, geraakt door deze wijzigingen. Ook het CBS, als bevoegd orgaan in het kader van hoofdstuk II van de Datagovernanceverordening, wordt mogelijk geraakt door de integratie van dit hoofdstuk in hoofdstuk VIIc van de Omnibus Digitaal.

De AVG zal voor (nagenoeg) alle uitvoeringsorganisaties relevant zijn omdat zij persoonsgegevens verwerken en voor sommige uitvoeringsorganisaties zal de AI-verordening relevant worden omdat zij met (hoog-risico) AI-systemen werken. Ook de opname van de Open Data Richtlijn in de Omnibus Digitaal heeft mogelijk

⁵ Zie overwegingen 41 en 43 van het voorstel voor de Digitale omnibus.

⁶ Kamerstukken II 2025/2026, 22112, nr. 4223

effect op uitvoeringsorganisaties. Het effect van wijzigingen aan deze wetten met als doel om regeldruk te verlagen zou beperkt moeten zijn, zeker als de wijzigingen in lijn met de kabinetsinzet focussen op versimpelen, verduidelijken en stroomlijnen.

9

Zijn deze uitvoeringsorganisaties geconsulteerd over de effecten die zijn voorzien voor de eigen organisatie en de gebruikers (burgers en bedrijven), en wat was hun visie/oordeel? Deze leden ontvangen graag een toelichting per uitvoeringsorganisatie.

Antwoord

Het kabinet betreft proactief de toezichthouders op de verschillende wetten. De AP heeft haar positie over de Omnibus Digitaal publiek bekend gemaakt.⁷ Het kabinet deelt de zorgen die de AP uit over o.a. het wijzigen van de definitie van persoonsgegevens en het schrappen van de registratieplicht voor bepaalde AI-systemen die in hoog-risico context worden ingezet. De ACM heeft aangegeven net als het kabinet kritisch te zijn op het intrekken van de P2B-verordening en werkt samen met het kabinet aan voorstellen om de Europese governance van datawetgeving via de Europese Raad voor Gegevensinnovatie (EDIB) te versterken.

De verschillende departementen betrekken hun uitvoeringsorganisaties bij de totstandkoming van het kabinetsstandpunt. Zoals aangegeven in de beantwoording van vraag 8 worden uitvoeringsorganisaties meer indirect geraakt door de omnibussen. Er is geen volledig overzicht van de oordelen van alle uitvoeringsorganisaties die persoonsgegevens verwerken. De zorgen over de impact van fundamentele wijzigingen aan de AVG zijn ook door sommige uitvoeringsorganisaties en medeoverheden geuit.

10

De leden van de fractie van GroenLinks-PvdA merken op dat de geopolitieke situatie aan grote veranderingen onderhevig is. In de huidige geopolitieke situatie is Nederlandse/Europese (digitale) autonomie een belangrijk speerpunt. Een agenda van deregulering, zoals de Omnibussen, met het oog op de vrije digitale markt, is in het voordeel van de grote (Amerikaanse) techbedrijven, zo menen de leden van de fractie van GroenLinks-PvdA. Wellicht vraagt de huidige situatie juist een tegengestelde beweging, namelijk van gerichtere (digitale) regulering in plaats van deregulering.

Hoe beoordeelt u de Omnibus Digitaal, de Omnibus AI en de Data Unie Strategie in de huidige geopolitieke situatie? Deze leden ontvangen graag een toelichting.

⁷ [Position paper AP: Omnibus Digitaal en Omnibus AI | Autoriteit Persoonsgegevens](#)

Antwoord

De voorstellen komen voort uit de Europese agenda voor betere regelgeving⁸. Deze agenda is onderdeel van het bredere plan om het concurrentievermogen van de EU te versterken, zoals uiteengezet door Commissievoorzitter Von der Leyen in haar politieke richtsnoeren voor de zittingsperiode 2024–2029. De Commissie geeft daarin aan, dat zoals benadrukt in het Draghi-rapport, de opeenstapeling van regels soms een negatief effect heeft gehad op het concurrentievermogen. Door de regeldruk van digitale regelgeving te verlagen zouden de voorstellen de concurrentiekracht moeten versterken.

Het verlagen van regeldruk is ook voor het kabinet een belangrijke prioriteit en het kabinet ziet net als de Europese Commissie dat dit kan bijdragen aan het versterken van het concurrentievermogen. Over de omnibussen als geheel verwacht het kabinet dat de omnibussen inderdaad de regeldruk verlagen door simplificatie en daarmee bijdragen aan het versterken van het concurrentievermogen. Zoals aangegeven in het BNC-fiche heeft het kabinet voor enkele onderdelen van de omnibussen heeft het kabinet wel vragen in hoeverre deze effectief de regeldruk verlagen.

Het kabinet oordeelt dat de Data Unie Strategie een positieve bijdrage kan leveren aan digitale autonomie. Pijler 3 van de strategie richt zich specifiek op veilige en betrouwbare internationale datastromen, waarin data als geopolitiek strategisch bezit wordt benaderd. Hierbij geldt: samenwerken waar (en met wie) het kan en beschermen waar nodig,.

11

Grondrechten in het geding

De leden van de fractie van GroenLinks-PvdA merken op dat het College voor de Rechten van de Mens is vastgesteld als grondrechtenautoriteit Artificiële Intelligentie (AI) in Nederland.⁹ De Omnibus Digitaal vormt volgens het College "een zorgwekkende ontwikkeling voor de bescherming van grondrechten, zoals het recht op non-discriminatie en gegevensbescherming".¹⁰

Kunt u een inhoudelijke reactie geven op deze uitspraak van het College voor de Rechten van de Mens?

Antwoord

Het kabinet deelt de opvatting van het College voor de Rechten van de Mens dat het van belang is om te onderzoeken hoe versimpeling kan plaatsvinden zonder onevenredige impact op grondrechten. Het kabinet ziet dat een aantal voorstellen voor aanpassingen aan de AVG een fundamentele impact kunnen hebben op grondrechten, waaronder het recht op gegevensbescherming. Het kabinet heeft de Commissie verzocht een uitgebreidere analyse van de impact van deze voorstellen

⁸ [Betere regelgeving - Europese Commissie](#)

⁹ College voor de Rechten van de Mens, 'College wordt grondrechtentoezichthouder Artificiële Intelligentie', 20 november 2024, <https://www.mensenrechten.nl/actueel/nieuws/2024/11/15/college-wordt-grondrechtentoezichthouder-artificiele-intelligentie>

¹⁰ [EU-wetswijzigingen 'digitale omnibus' zorgelijk voor grondrechten | College voor de Rechten van de Mens](#)

te presenteren. Het kabinet heeft daarnaast aangegeven dat het advies van de EDPS en het EDPB, dat 10 februari is vastgesteld, moet worden betrokken bij de bespreking van dit voorstel. Daarmee zet het kabinet erop in de voorstellen die verdergaan dan versimpeling te behandelen op een wijze die recht doet aan de potentiële impact en de zorgpunten.

12

Kunt u een overzicht geven van alle potentiële aantastingen van grondrechten (uit de Nederlandse Grondwet en Europese wetgeving) die in het geding zijn? Kunt u deze uiteenzetting duidelijk relateren aan de voorgestelde wijzigingen? Deze leden verzoeken u hierbij speciale aandacht te besteden aan artikel 8 van het Handvest van de grondrechten van de Europese Unie.

Antwoord

Zoals aangegeven in het BNC-fiche¹¹, is één van de voorgestelde wijzigingen aan de AVG die de meeste impact lijkt te hebben op het beschermingsniveau van het grondrecht op gegevensbescherming de wijziging van de definitie van het begrip persoonsgegevens. Dit begrip bepaalt immers of de AVG – en alle rechten van betrokkenen – van toepassing is. Dat deze wijziging de meeste impact zou hebben, is inmiddels bevestigd in het advies van de EDPB en EDPS van 10 februari. Zij stellen dat deze wijziging zou leiden tot een aanzienlijke beperking van de reikwijdte van het begrip persoonsgegevens en daarmee van de reikwijdte van de AVG. De EDPB en EDPS adviseren nadrukkelijk om de wijziging van deze definitie niet te aanvaarden. Er lijkt voldoende steun in de Raad om deze wijziging terug te draaien.

Een andere wijziging die impactvol lijkt te zijn, is het voorstel voor het creëren van grondslagen voor het verwerken van (met name bijzondere) persoonsgegevens voor het trainen en exploiteren van AI-systemen. Dit voorstel lijkt nu vast te leggen dat bij de training en exploitatie van een AI-model de grondslag 'gerechtvaardigd belang' per definitie is gegeven, zonder dat daarvoor een noodzakelijkheidstoets en de bijbehorende belangenafweging noodzakelijk is. Het kabinet acht een noodzakelijkheidstoets en de bijbehorende belangenafweging bij de toepassing van de grondslag gerechtvaardigd belang echter essentieel om de grondrechten van burgers te waarborgen.

Het voorstel voorziet daarnaast ook in een uitzondering op het verbod op de verwerking van bijzondere categorieën van persoonsgegevens voor het trainen en exploiteren van AI-systemen; ook dit is een voorbeeld van een wijziging met mogelijk grote impact op het beschermingsniveau. Zoals ook uiteengezet in het BNC-fiche, genieten bijzondere persoonsgegevens juist extra bescherming vanwege de gevolgen die de verwerking van deze bijzondere categorieën van persoonsgegevens voor de betrokkenen kunnen hebben. Wanneer deze gegevens mogen worden verwerkt voor genoemd doel, is het extra belangrijk dat er goede randvoorwaarden zijn. Verruiming van deze bevoegdheden zou alleen aan de orde

¹¹: Kamerstukken II 2025/2026, 22112, nr. 4223

kunnen zijn als de bescherming van fundamentele rechten voldoende gewaarborgd is.

Het voorstel voorziet ook in een grondslag voor de verwerking van bijzondere persoonsgegevens voor het detecteren en corrigeren van bias voor alle AI-systemen. In de huidige tekst van de AI-verordening is deze wettelijke grondslag alleen van toepassing op *hoog-risico* AI-systemen. Ook hiervoor geldt dat dit alleen aan de orde zou kunnen zijn als de fundamentele rechten voldoende gewaarborgd zijn en de risico's proportioneel zijn tot het doel van detecteren en corrigeren van bias. Het detecteren en corrigeren van bias in AI-systemen kan het non-discriminatierecht juist versterken.

De EDPB en EDPS stellen in hun advies van 10 februari jl. dat de voorgestelde bepalingen over de verwerking van bijzondere persoonsgegevens in AI-context op tal van punten verbetering behoeven, onder meer om het toepassingsgebied ervan te verduidelijken en om noodzakelijke waarborgen toe te voegen.¹²

13

Ondernemingsklimaat

De leden van de fractie van GroenLinks-PvdA merken op dat er niet één allesomvattend optimaal ondernemingsklimaat bestaat dat voor alle typen bedrijven even gunstig is.

Ziet u een spanningsveld tussen de belangen van het Midden- en Kleinbedrijf (MKB) in Nederland en Europa enerzijds en grote (Amerikaanse) techbedrijven anderzijds in deze voorstellen? In hoeverre worden grote spelers bevoordeeld ten opzichte van het MKB? Deze leden ontvangen graag een toelichting.

Antwoord

Het kabinet erkent dat kleinere bedrijven andere uitdagingen ervaren dan grote bedrijven met betrekking tot regeldruk. Grotere bedrijven zijn over het algemeen beter in staat dan kleine bedrijven om complexe regelgeving zelfstandig te interpreteren en toe te passen. Kleinere bedrijven hebben baat bij heldere regels en ondersteuning die het makkelijker maakt regels na te leven.

Zowel binnen de nationale als de Europese agenda voor betere regelgeving¹³ is daarom bijzondere aandacht voor het mkb. De omnibussen zijn onderdeel van de agenda voor betere regelgeving en bevatten daarom verschillende aanpassingen die er specifiek op zijn gericht naleving van de regels door mkb of small midcapbedrijven makkelijker te maken. Daarnaast zorgt met name de Omnibus AI ervoor dat er meer richtsnoeren worden ontwikkeld, die het makkelijker maken aan de regels te voldoen.

Het kabinet geeft in het BNC-fiche aan dat een aantal voorstellen uit de omnibussen mogelijk niet effectief de regeldruk verlagen. Bij verschillende van

¹² [Digitale omnibus: EDPB en EDPS ondersteunen vereenvoudiging en concurrentievermogen en maken zich grote zorgen | European Data Protection Board](#)

¹³ [Betere regelgeving - Europese Commissie](#)

deze voorstellen - zoals het Europees meldpunt, bepaalde wijzigingen aan de AVG en de uitzonderingen in de Dataverordening op de bepalingen over overstappen tussen clouddiensten - verwacht het kabinet dat deze met name voor het mkb geen lastenverlichting zullen opleveren. Deze voorstellen lijken de complexiteit van (het naleven van) wetgeving te verhogen of creëren complexe uitzonderingen waar kleinere bedrijven waarschijnlijk minder snel gebruik van zullen maken.

14

Bent u van mening dat de Digitale Omnibus, de Omnibus AI en de Data Unie Strategie eerlijke concurrentie waarborgen? Of wordt er een rode loper uitgelegd voor de verdienmodellen van grote (Amerikaanse) techbedrijven ten koste van de privacy? Deze leden ontvangen graag een toelichting.

Antwoord

Het kabinet kan veel voorgestelde aanpassingen binnen de omnibussen steunen, omdat deze in lijn met de kabinetsinzet wetgeving versimpelen, verduidelijken en stroomlijnen. Voor deze voorstellen verwacht het kabinet dat deze ook eerlijke concurrentie waarborgen. Zoals aangegeven in de beantwoording van vraag 13 en het BNC-fiche heeft het kabinet bij enkele wijzigingen zorgen dat deze de bescherming van (privacy)grondrechten mogelijk verzwakken en niet bijdragen aan het verlagen van regeldruk. Sommige voorstellen lijken de complexiteit van (het naleven van) wetgeving voor met name kleine bedrijven te verhogen of creëren complexe uitzonderingen waar kleinere bedrijven waarschijnlijk minder snel gebruik van zullen maken. Het kabinet zet erop in deze voorstellen te verbeteren zodat deze effectief bijdragen aan het versimpelen van digitale wetgeving, zonder daarbij afbreuk te doen aan de doelen van de wetgeving.

15

Ziet u mogelijk nog andere effecten die voor verschillende groepen ondernemers anders uitwerken? Deze leden ontvangen graag een toelichting.

Antwoord

Het primaire effect van de omnibussen is het verlagen van regeldruk. Omdat de wetten die worden gewijzigd zich richten op digitale technologieën en diensten zullen de voorstellen in het algemeen meer impact hebben op bedrijven die meer gedigitaliseerd zijn, met AI werken of veel data verwerken. Behalve deze verschillen en de in de beantwoording op vraag 13 en 14 aangegeven effecten zie het kabinet geen noemenswaardige verschillen tussen groepen ondernemers.

16

European Digital Rights (EDRI) stelt dat de 'vereenvoudiging' nieuwe complexiteit introduceert en dat grote bedrijven de juridische afdelingen hebben om deze mazen in de wet op te zoeken, terwijl het MKB in onzekerheid achterblijft.¹⁴ Kunt u hierop reflecteren?

¹⁴ ICS, 'The Digital Omnibus: Simplifying Europe's Digital Rulebook and Its Impact on Ireland', 26 november 2025, <https://ics.ie/2025/11/26/the-digital-omnibus-simplifying-europes-digital-rulebook-and-its-impact-on-ireland/>

Antwoord

Zoals aangegeven in de beantwoording van vraag 13 en vraag 14 ziet het kabinet dat veel voorgestelde aanpassingen wetgeving versimpelen, verduidelijken en stroomlijnen, ook voor het mkb. Voor een aantal voorgestelde aanpassingen - zoals het Europees meldpunt en de gewijzigde definitie van persoonsgegevens - verwacht het kabinet dat deze met name voor het mkb geen lastenverlichting zullen opleveren.

17

De leden van de fractie van GroenLinks-PvdA lezen dat grote techbedrijven ruim 150 miljoen per jaar uitgeven aan de lobby voor hun belangen in Europa.¹⁵ Heeft u zicht op deze lobby? Hoe beoordeelt u de invloed van deze lobby, waarbij vertraging, versoepeling en herformulering een belangrijke rol speelt bij de totstandkoming van de voorstellen? Deze leden ontvangen graag een toelichting.

Antwoord

Net als vele andere stakeholders lobbyen grote techbedrijven actief bij de totstandkoming van digitale wetgeving. Het is gebruikelijk dat overheden input van stakeholders gebruiken bij het opstellen van beleid en wetgeving. Het is wel van belang dat hierbij een brede en diverse groep stakeholders wordt geconsulteerd.

Het kabinet ziet dat ook bij de totstandkoming van deze voorstellen een brede groep stakeholders is geconsulteerd. In het SWD dat tegelijk met de omnibusvoorstellen is gepresenteerd¹⁶ geeft de Commissie onder andere in Annex I inzicht welke stakeholders het heeft geconsulteerd. Dit betreft een brede groep stakeholders, variërend van burgerrechtenorganisaties tot grote techbedrijven. Het kabinet ziet niet dat grote techbedrijven een onevenredige invloed op deze voorstellen hebben gehad. Sommige techbedrijven en belangengroepen die techbedrijven vertegenwoordigen hebben ook aangegeven niet tevreden zijn met de omnibussen.¹⁷

18

De leden van de fractie van GroenLinks-PvdA lezen dat Corporate Europe Observatory de invloed van de lobby van grote (Amerikaanse) techbedrijven op verschillende artikelen van de Omnibus Digitaal heeft geanalyseerd.¹⁸ Kunt u reflecteren op de analyse van Corporate Europe Observatory?

¹⁵ Digwatch, 'Big Tech ramps up Brussels lobbying as EU considers easing digital rules', 30 oktober 2025, <https://dig.watch/updates/big-tech-ramps-up-brussels-lobbying-as-eu-considers-easing-digital-rules#:~:text=Spending%20is%20concentrated%20among%20US,so%2C%20ask%20our%20Diplo%20chatbot>

¹⁶ SWD(2025) 836 final

¹⁷ [Digital omnibus: a first step and what must come next, now - DIGITALEUROPE](#)

¹⁸ Corporate Europe Observatory, 'Article by article, how Big Tech shaped the EU's roll-back of digital rights', 14 januari 2026, <https://corporateeurope.org/en/2026/01/article-article-how-big-tech-shaped-eus-roll-back-digital-rights>

Antwoord

De voorgestelde wijzigingen die in het artikel¹⁹ worden benoemd zijn over het algemeen wijzigingen waar het kabinet kritisch op is of zorgen over heeft omdat ze doelen van de wetgeving afzwakken, afbreuk doen aan het niveau van gegevensbescherming en in veel gevallen niet lijken bij te dragen aan het verlagen van de regeldruk. Dit is in het BNC-fiche over de voorstellen toegelicht.

19

In het kader van transparantie is het belangrijk om ook zicht te hebben op de lobby in Nederland. Welke contacten heeft de Nederlandse regering en/of de ambtelijke ondersteuning gehad met lobbyisten van techbedrijven om de standpunten te bepalen? Deze leden ontvangen graag een toelichting.

Antwoord

Zoals gebruikelijk heeft het kabinet bij en sinds de totstandkoming van het kabinetsstandpunt contact met een brede groep stakeholders. Ambtelijk is er in dat kader ook contact geweest met techbedrijven. Naar mijn weten zijn er voor de totstandkoming van het kabinetsstandpunt op politiek niveau geen gesprekken geweest met lobbyisten van grote Amerikaanse techbedrijven specifiek over deze omnibussen.

20

Wijzigingen bevoegdheden

De leden van de fractie van GroenLinks-PvdA wijzen erop dat de in de Omnibus Digitaal voorgestelde bevoegdheden voor de Commissie om op grond van de AVG een aantal uitvoeringshandelingen vast te stellen, leidt tot een verschuiving van bevoegdheden van de onafhankelijke toezichthouders en de EDPB naar de Europese Commissie. Het betreft bevoegdheden voor de Europese Commissie om standaarden voor datalekmeldingen en omschrijving van hoog risico gevallen voor datalekken vast te stellen (art. 3, lid 8, sub c), om uitvoeringshandelingen vast te stellen over de gevallen waarin Data Protection Impact Assessments (DPIA's) verplicht zijn (art. 3, lid 9, sub b) en om uitvoeringshandelingen vast te stellen om criteria en middelen te omschrijven om zo te bepalen wanneer er geen sprake meer is van persoonsgegevens bij pseudonimisering (art. 3, lid 10). In het BNC-fiche lezen deze leden dat de regering "hier een risico ziet van meer politieke besluitvorming, wat niet vanzelfsprekend past bij een verordening die mede strekt tot grondrechtenbescherming". Deze leden zien dit risico ook en vinden dit een zeer onwenselijke ontwikkeling. Deze leden lezen voorts in het BNC-fiche dat het toekennen van de bevoegdheid van artikel 3, lid 10 van het voorstel aan de Commissie "niet mogelijk" is volgens de regering. Omdat deze uitvoeringshandelingen die de Commissie op basis van dit artikel zou kunnen vaststellen betrekking hebben op de definitie van persoonsgegevens (artikel 41a), betreft dit een essentieel onderdeel van de basishandeling, dat zich "niet leent" voor uitwerking in uitvoeringshandelingen, aldus de regering. Dergelijke uitvoeringshandelingen zouden bovendien mogelijk betrekking hebben op de reikwijdte van het grondrecht op bescherming van persoonsgegevens. De AVG is

¹⁹ Article by article, how Big Tech shaped the EU's roll-back of digital rights | Corporate Europe Observatory

immers een uitwerking van het recht op gegevensbescherming. Daarnaast krijgt de Commissie in artikel 1, lid 25, sub c, van het voorstel de bevoegdheid om uitvoeringshandelingen vast te stellen waarin handhavingsbevoegdheden van de Europese Commissie worden bepaald, waaronder het opleggen van boetes en andere sancties (wijziging van artikel 75 van de AI-verordening). Ook het toekennen van deze bevoegdheid om handhavingsbevoegdheden vast te stellen is "niet mogelijk" volgens de regering. De regering acht het toekennen van handhavingsbevoegdheden aan de Europese Commissie, waarbij een evenwicht moet worden gevonden tussen de uiteenlopende belangen die aan de orde zijn, "niet acceptabel".

Er worden in het BNC-fiche verschillende termen gebruikt om de wijziging van de bevoegdheden van de Europese Commissie te duiden, waaronder "niet leent", "niet acceptabel" en "niet mogelijk". Kunt u een preciezer juridisch oordeel geven over alle voorgestelde wijzigingen van de bevoegdheden? Deze leden ontvangen daarbij graag per wijziging van bevoegdheid een afzonderlijk oordeel, evenals een nadere juridische duiding van het mogelijk effect op de reikwijdte van het recht op bescherming van persoonsgegevens.

Antwoord

Het kabinet brengt de zorgen over de verschuiving van bevoegdheden naar de Commissie – zoals omschreven in het BNC-fiche – naar voren tijdens de onderhandelingen en pleit voor behoud van deze bevoegdheden voor de EDPB. Het kabinet voelt zich hierin onder meer gesterkt door het advies van de EDPB en EDPS van 10 februari jl., die hebben aanbevolen om de Commissie geen rol te geven bij de vaststelling van de lijsten over wanneer DPIA's of meldingen van datalekken verplicht zijn, en ook niet bij criteria inzake pseudonimisering. Er lijkt voldoende steun in de Raad om deze bevoegdheden voor de EDPB te behouden.

Voor elk van deze bepalingen geldt dat zij volgens het kabinet niet in lijn zijn met de onderlinge verhoudingen tussen de organen van de EU, het stelsel van toezicht en de scheiding der machten. Voor wat betreft de uitvoeringshandelingen inzake pseudonimisering op grond van het voorgestelde artikel 41a AVG is bovendien van belang dat fundamentele rechten volgens jurisprudentie van het Hof van Justitie van de EU (HvJEU) niet kunnen worden beperkt door middel van uitvoeringshandelingen.²⁰ Met het voorgestelde artikel 41a AVG zou daarvan sprake kunnen zijn omdat de uitvoeringshandelingen verband zouden houden met de definitie van persoonsgegevens en aldus feitelijk het toepassingsbereik van de AVG zouden bepalen, doordat pseudonimisering zou worden gebruikt om aan te tonen dat de AVG niet van toepassing is.

21

Wat is uw strategie om dit onderdeel van de Omnibus Digitaal aangepast te krijgen?

Antwoord

²⁰ Hof van Justitie van de EU 5 september 2012 (Europees Parlement / Raad), C-355/10, rechtsoverweging 77.

Hiervoor verwijs ik u graag naar het antwoord op vraag 20. Er lijkt voldoende steun in de Raad om deze bevoegdheden voor de EDPB te behouden.

22

Hoe ligt het Europese krachtenveld ten aanzien van deze aanpassingen?

Antwoord

Zoals aangegeven in het antwoord op vraag 20 lijkt er voldoende steun in de Raad om deze bevoegdheden voor de EDPB te behouden.

23

Is aanpassing van dit onderdeel een harde randvoorwaarde om in te kunnen stemmen met de Omnibus Digitaal?

Antwoord

Het kabinet zal op basis van het uiteindelijke onderhandelingsresultaat beoordelen of de omnibus als geheel voldoende in lijn is met de Nederlandse inzet. De inzet van het kabinet is om deze bevoegdheden niet bij de Commissie te beleggen en dit zal een (belangrijke) factor zijn in het beoordelen van het totale voorstel.

24

Nationale veiligheid

De leden van de fractie van GroenLinks-PvdA merken op dat door de inrichting van een Europees meldpunt een deel van de nationale dienstverlening rondom incidentenafhandeling verschuift naar Europees niveau. Dit geldt ook voor meldingen onder de NIS2 en CER, waar incidenten bij de Rijksoverheid en vitale infrastructuur gevoelige informatie omtrent nationale veiligheid kunnen bevatten. In het BNC-fiche wordt benadrukt dat "nationale meldstructuren, waarbij lidstaten de directe en primaire ontvanger van incidentinformatie blijven, behouden moeten blijven". Ook staat in het BNC-fiche dat de regering daarnaast zorgen heeft "omtrent beveiligingsrisico's als het gaat om het centraliseren van dergelijke meldplichten binnen één meldpunt. Het verwerken van zeer gevoelige meldingen, en in het bijzonder incidentinformatie van 27 lidstaten is namelijk erg kwetsbaar en een zaak van nationale veiligheid. Daarbij ziet het kabinet ook risico's ten aanzien van de afhankelijkheid van de continuïteit van een platform dat op EU-niveau wordt beheerd".

Kunt u nader toelichten welke kwetsbaarheden in het kader van de (nationale) veiligheid voorzien worden?

Antwoord

Het kabinet acht het van belang om te melden dat de meldplicht als bedoeld in de NIS2-richtlijn alleen geldt voor significante incidenten. Een incident is significant als het een ernstige operationele verstoring van de diensten of financiële verliezen voor de betrokken entiteit veroorzaakt of kan veroorzaken óf andere entiteiten heeft getroffen of kan treffen door aanzienlijke materiële of immateriële schade te veroorzaken. Dit betekent dat de inhoud van de gedane meldingen gevoelige informatie zal kunnen bevatten, die mogelijk ook de nationale veiligheid kan raken. Deze meldingen zullen, na inwerkingtreding van de Cyberbeveiligingswet,

moeten worden gedaan bij zowel het CSIRT als de bevoegde autoriteit. Hiervoor zal door de Minister van Justitie en Veiligheid een meldpunt worden ingericht, waarbij ook de nodige waarborgen zijn ingebouwd om op een veilige manier de meldingsinformatie te ontvangen.

Het kabinet acht het centraliseren van de meldplicht binnen één Europees meldpunt kwetsbaar, omdat het voor kwaadwillenden, ingeval zij erin slagen ongeoorloofde toegang te krijgen tot dit Europese meldpunt, op deze wijze mogelijk is om op Europese – en daarmee grote – schaal inzicht te krijgen in de meldingen van 27 lidstaten. Op deze wijze kan de verkregen gebundelde informatie uitgebuit worden en de continuïteit van een platform dat op EU-niveau wordt beheerd in gevaar worden gebracht. Dit maakt niet alleen onze digitale veiligheid, maar ook onze nationale veiligheid kwetsbaar.

25

Wat is uw strategie om dit onderdeel van de Omnibus Digitaal aangepast te krijgen?

Antwoord

Het kabinet zal zich inspannen om te bezien of het oprichten, beheren en beveiligen van een meldpunt voor verschillende soorten wetgeving past binnen het mandaat, de capaciteit en de verantwoordelijkheid van ENISA. Daarnaast zal het kabinet binnen de onderhandelingen de voordelen en mogelijkheden van het nationaal in te richten meldpunt benadrukken en aansluiting zoeken bij lidstaten met een vergelijkbare positie.

26

Hoe ligt het Europese krachtenveld rondom deze aanpassingen?

Antwoord

Het kabinet verwacht dat een aantal lidstaten zorgen zal uiten over de oprichting van een Europees meldpunt. Het kabinet zal zich tijdens de onderhandelingen verder inspannen om aansluiting te zoeken bij lidstaten met een vergelijkbare positie.

27

Is aanpassing van dit onderdeel een harde randvoorwaarde om in te kunnen stemmen met de Omnibus Digitaal?

Antwoord

Het Kabinet kan vooralsnog geen uitspraak doen over de instemming aangezien de onderhandelingen nog lopen en er nog vragen zijn gesteld over de geschiktheid van dit onderdeel, in het licht van de verlaging van de regeldruk. Het kabinet verwacht namelijk dat het verlagen van regeldruk meer efficiënt en tijdig kan worden bereikt door voort te bouwen op bestaande nationale oplossingen in plaats van het organiseren van een Europees meldpunt. Nationale meldstructuren en meldpunten sluiten aan bij de manier van samenwerken en communiceren die entiteiten hebben met de Nederlandse overheid. Het kabinet zal zich actief inzetten voor het behoud van deze nationale meldstructuren.

28

In het kader van de proportionaliteitsbeoordeling lezen deze leden in het BNC-fiche dat de regering vraagtekens heeft over de proportionaliteit van de voorstellen ten aanzien van een Europees meldpunt: "De tweede kanttekening is dat het kabinet zorgen heeft ten aanzien van de inrichting van een Europees meldpunt. Volgens het kabinet is door de Commissie onvoldoende inzichtelijk gemaakt of een Europees meldpunt daadwerkelijk zal zorgen voor lastenverlichting en simplificatie, in het bijzonder waar het gaat om niet-grensoverschrijdende entiteiten. Ook is onvoldoende duidelijk wat de omvang is van de groep entiteiten die wel voordeel zouden kunnen hebben bij een Europees meldpunt, namelijk de grensoverschrijdende entiteiten en/of (grensoverschrijdende) entiteiten die rapportageverplichtingen hebben die onder meerdere wetgevingskaders vallen, bijvoorbeeld AVG én NIS2-richtlijn. Om die reden heeft het kabinet twijfels over de geschiktheid van deze maatregel in het licht van het doel om regeldruk te verlagen".

Is er inmiddels meer helderheid over de geconstateerde onduidelijkheden?

Antwoord

Over de geconstateerde onduidelijkheden is nog geen helderheid verkregen; wij hopen dat het verdere onderhandelingsproces hierin duidelijkheid zal verschaffen.

29

Heeft u een nader oordeel over de proportionaliteit van dit onderdeel?

Antwoord

Het kabinet twijfelt nog steeds over de geschiktheid van een Europees meldpunt om de regeldruk te verlagen. Het kabinet acht het oprichten van een Europees meldpunt niet proportioneel en gaat bovendien verder dan wat nodig is om de beoogde doelstelling te verwezenlijken: het kabinet verwacht dat het verlagen van regeldruk meer efficiënt en tijdig kan worden bereikt door voort te bouwen op bestaande nationale meldpunten in plaats van het organiseren van een Europees meldpunt. Zo wordt op nationaal niveau al gewerkt aan harmonisatie van de inrichting van de meldplicht, en daarmee het beperken van de regeldruk, voor de NIS2 en CER-meldingen.

30

Uitstellen verplichtingen met betrekking tot hoog risico AI-systemen
De EDPB en de EDPS hebben in een gezamenlijke opinie over de Omnibus AI gepleit om de verplichtingen volgens de oorspronkelijke planning in te laten gaan. De leden van de fractie van GroenLinks-PvdA maken zich, gezien de razendsnelle ontwikkelingen van AI -systemen, zorgen over het uitstellen van de verplichtingen met betrekking tot hoog risico AI -systemen. Met deze voorstellen worden verplichtingen met respectievelijk zestien maanden en twaalf maanden vertraagd, waarbij de inwerkingtreding wordt gekoppeld aan een Commissiebesluit.

Hoe oordeelt u over dit advies van de EDPB en de EDPS? Deze leden ontvangen graag een toelichting.

Antwoord

Zoals aangegeven in het non-paper over regeldruk en digitale wetgeving, heeft het kabinet de voorkeur dat er spoedig ondersteuningsmiddelen worden ontwikkeld om te verduidelijken wat nodig is om aan de verplichtingen uit de AI-verordening te voldoen, dan dat inwerkingtreding wordt uitgesteld. De ontwikkeling van deze ondersteuningsmiddelen duurt echter langer dan voorzien. Dat is een belangrijke reden dat de Europese Commissie de inwerkingtreding van de verplichtingen heeft uitgesteld.

31

Deelt u de zorgen van deze leden? Zo nee, waarom niet?

Antwoord

Het kabinet ziet liever korter uitstel voor hoog-risico AI-systemen in bijlage III. Er lijkt in de Raad onvoldoende steun om het uitstel van de inwerkingtreding van deze bepalingen te verkorten. Alhoewel het kabinet een voorkeur heeft voor korter uitstel van de inwerkingtreding van deze bepalingen, ziet zij ook dat deze bepalingen niet effectief de risico's van AI-systemen inperken als voor organisaties onduidelijk is hoe ze aan de verplichtingen moeten voldoen. Met name kleinere organisaties hebben ondersteuning nodig om te kunnen voldoen aan de verplichtingen voor hoog-risico AI-systemen, bijvoorbeeld in de vorm van standaarden en richtsnoeren.

32

Kunt u een inschatting maken van de mogelijke effecten, waaronder op ondernemers die door deze aanpassing geen vaste invoeringsdatum kennen?

Antwoord

Het kabinet zet erop in dat wordt vastgehouden aan vaste data voor inwerkingtreding van de bepalingen voor hoog-risico AI. De koppeling van inwerkingtreding aan een Commissiebesluit brengt onzekerheid met zich mee. Hiervoor lijkt voldoende steun in de Raad. Zoals aangegeven in de beantwoording van vraag 31 ziet het kabinet dat deze bepalingen niet effectief de risico's van AI-systemen inperken als voor organisaties onduidelijk is hoe ze aan de verplichtingen moeten voldoen. Met name kleinere organisaties hebben ondersteuning nodig om te kunnen voldoen aan de verplichtingen voor hoog-risico AI-systemen, bijvoorbeeld in de vorm van standaarden en richtsnoeren.

33

Hoe ligt het Europese krachtenveld ten aanzien van deze aanpassingen?

Antwoord

Er lijkt voldoende steun in de Raad voor vaste data voor inwerkingtreding van de bepalingen over hoog-risico AI. Er lijkt brede steun onder lidstaten om de inwerkingtreding van de bepalingen over hoog-risico AI, zoals voorgesteld door de Commissie, met 12 en 16 maanden uit te stellen.

34

Is aanpassing van dit onderdeel een harde randvoorwaarde om in te kunnen stemmen met de Omnibus AI?

Antwoord

Het kabinet zal op basis van het uiteindelijke onderhandelingsresultaat beoordelen of de omnibus als geheel voldoende in lijn is met de Nederlandse inzet.

35

Past deze aanpassing in de actuele strategie om minder afhankelijk te worden van de grote (Amerikaanse) techbedrijven? Deze leden ontvangen graag een toelichting.

Antwoord

Met name voor kleinere organisaties in de EU levert het moeten voldoen aan de eisen uit de AI-verordening een extra last op. Zij zijn daarbij afhankelijk van de beschikbaarheid van technische standaarden, die op dit moment nog niet af zijn. Grote techbedrijven hebben relatief meer middelen tot hun beschikking om te kunnen voldoen aan (nieuwe) wetgeving dan kleinere (Europese) organisaties.

Het kabinet is daarom niet per definitie tegen uitstel van de hoog-risico eisen. Het is daarbij wel belangrijk dat dit op een duidelijke en transparante manier gebeurt, zodat organisaties in de EU weten waar ze aan toe zijn.

36

Deze leden horen veel zorgen over de zogenaamde AI-gedreven 'nudifier' tools. Deelt u deze zorgen? Zo nee, waarom niet?

Antwoord

Ja, deze zorgen deel ik. Het is schrijnend dat met AI gedreven uitkleed tools op grote schaal deepnudes worden gegenereerd. Dat veel mensen, met name vrouwen en minderjarigen, slachtoffer zijn geworden is zorgwekkend.

37

Is de regering bereid om in Europa te pleiten voor een verbod op deze tools, bijvoorbeeld in artikel 5 van de AI-verordening?

Antwoord

Er is nog weinig bekend over de effectiviteit van een mogelijk verbod, de wijze waarop dit vorm kan krijgen en de handhavingsmogelijkheden. Binnen het ministerie van Justitie en Veiligheid wordt gekeken naar de mogelijkheden om het gebruik van nudify applicaties verder tegen te gaan. Hierbij wordt ook bezien of het wenselijk en haalbaar is om het aanbieden van de applicaties zelf te verbieden, nationaal dan wel Europees, zoals bijvoorbeeld via de AI-verordening.

38

De EDPB en de EDPS hebben in een gezamenlijke opinie over de Omnibus AI gepleit om de voorgenomen aanpassingen van de registratieplicht van hoog risico AI-systemen niet door te voeren omdat dit transparantie en toezicht ondermijnt en misbruik in de hand kan werken.

In het BNC-fiche lezen deze leden dat de regering bezwaren heeft "tegen het schrappen van de registratieplicht voor hoog-risico AI die alleen voor beperkte of procedurele taken worden gebruikt. Dit de transparantie verlaagt over het gebruik van AI-systemen in hoog risico context en bemoeilijkt het toezicht op deze systemen. Bovendien levert deze maatregel slechts een beperkte verlichting van regeldruk op".

Hoe oordeelt u over het advies van de EDPB en de EDPS? Deze leden ontvangen graag een toelichting.

Antwoord

De EDPB en de EDPS benadrukken in hun opinie dat de registratie van systemen waarvan de aanbieder oordeelt dat deze slechts een bijkomende functie hebben en daarom geen hoog-risico AI-systeem zijn, een belangrijke bron is voor toezichthouders in het kader van hun toezicht. Indien deze registratieplicht verdwijnt, zullen toezichthouders meer middelen moeten inzetten om te achterhalen waar in de samenleving deze AI-systemen worden gebruikt.

Tegelijkertijd benoemen de EDPB en de EDPS dat het registreren van deze AI-systemen een verplichting met een zeer beperkte last is, zeker omdat de aanbieder wel nog steeds intern het oordeel dat een AI-systeem niet hoog-risico is moet documenteren.

Het kabinet deelt deze lezing van de EDPB en de EDPS. De zorgen over het schrappen van de registratieplicht en de beperkte lastenverlichting zijn beide genoemd in het BNC-fiche van het kabinet.

39

Wat is uw proportionaliteitsoordeel op dit onderdeel?

Antwoord

Zoals aangegeven in het antwoord op vraag 38 ziet het kabinet dat dit onderdeel slechts beperkte lastenverlichting oplevert en wel het toezicht op bepaalde AI-systemen, die mogelijk een hoog-risico vormen, aanzienlijk bemoeilijkt. Het kabinet ziet deze specifieke voorgestelde maatregel daarom als disproportioneel.

40

Kunt u een nadere toelichting geven op de wijze waarop het toezicht bemoeilijkt wordt en wat de gevolgen daarvan kunnen zijn?

Antwoord

Zoals aangegeven in beantwoording van vraag 38 is de registratie van systemen waarvan de aanbieder oordeelt dat deze slechts een bijkomende functie hebben en daarom geen hoog-risico AI-systeem zijn, een belangrijke bron voor toezichthouders in het kader van hun toezicht. Indien deze registratieplicht verdwijnt, zullen toezichthouders meer middelen moeten inzetten om te achterhalen waar in de samenleving deze AI-systemen worden gebruikt. Toezichthouders hebben daardoor minder zicht op aanbieders van deze AI-

systemen terecht concluderen dat het AI-systeem geen hoog-risico vormt, ondanks dat het in een hoog-risico context wordt gebruikt.

41

Wat is uw strategie om dit onderdeel van de Digitale Omnibussen aangepast te krijgen?

Antwoord

Het kabinet pleit voor behoud van deze registratieplicht.

42

Hoe ligt het Europese krachtenveld ten aanzien van deze aanpassingen?

Antwoord

Er lijkt voldoende steun in de Raad om deze registratieplicht in stand te houden.

43

Is aanpassing van dit onderdeel een harde randvoorwaarde voor u om in te kunnen stemmen met de Omnibus AI?

Antwoord

Het kabinet zal de uiteindelijke Omnibus AI in zijn geheel wegen en op basis daarvan bepalen of zij met de Omnibus AI kan instemmen. Het kabinet is positief over de verwachte Raadspositie, waarin deze registratieplicht waarschijnlijk in stand zal blijven.

44

De laatste maanden is er veel te doen over digitale autonomie en minder afhankelijkheid van de grote (Amerikaanse) techbedrijven. Past deze aanpassing in de actuele strategie om minder afhankelijk te worden van de grote (Amerikaanse) techbedrijven? Deze leden ontvangen graag een toelichting.

Antwoord

Zoals aangegeven in het antwoord op vragen 38 tot en met 43, ziet het kabinet het schrappen van deze registratieplicht als een beperkte lastenverlichting die niet opweegt tegen het verminderen van de transparantie bij deze AI-systemen. Deze aanpassing heeft daarmee een beperkte invloed op het concurrentievermogen van Europese organisaties en deze maatregel is ook minder relevant voor het versterken van de digitale open strategische autonomie.

45

De leden van de fractie van GroenLinks-PvdA merken op dat het belangrijk is om een goed niveau van toezicht te borgen. De EDPB en EDPS uiten zorgen over de positie van de nationale toezichthouders (o.a. verlies bevoegdheden en onafhankelijkheid) en de taakafbakening van en de samenwerking met het AI-bureau. Ook zijn er grote zorgen over het gebrek aan capaciteit bij zowel de nationale toezichthouders als het AI-bureau om duizenden bedrijven te controleren op wat er "onder de motorkap" van een AI-systeem gebeurt.

Hoe oordeelt u over de zorgen van de EDPB en EDPS? Deze leden ontvangen graag een toelichting.

Antwoord

Het kabinet zet in op een duidelijke afbakening van de taken van het AI Bureau. Voor wat betreft de capaciteit voor toezichthouders is in het algemeen van belang dat er voldoende capaciteit beschikbaar is voor toezichthouders. Specifiek voor de AI-verordening moet de structurele benodigde capaciteit voor toezicht op de AI-verordening in Nederland nog worden vastgesteld en toegekend.

Het kabinet is actief met de aan te wijzen toezichthouders in gesprek om te bepalen wat de benodigde middelen zijn voor de uitvoering van het toezicht. Bij het starten van de internetconsultatie van de Nederlandse uitvoeringswet voor AI-verordening, waar de bevoegdheden en taken van de toezichthouders in zijn vastgelegd, worden de voorgestelde toezichthouders gevraagd uitvoerings- en handhavingstoetsen op te stellen. Hiermee krijgt het kabinet een nog duidelijker beeld van de capaciteit die nationaal benodigd is voor de toezichthoudende taak.

46

Wat is volgens u nodig aan capaciteit (nationaal en Europees) om de toezichthoudende taak goed uit te voeren? Deze leden ontvangen graag een toelichting.

Antwoord

In het SWD geeft de Commissie aan 50 extra FTE nodig te hebben voor de voorgestelde aangepaste toezichthoudende taken. Het kabinet ziet dit op basis van de informatie in het SWD in principe als een realistische inschatting. Wel is het daarbij belangrijk dat de bevoegdheid van de Commissie duidelijk is afgebakend.

Op nationaal niveau is het kabinet zoals aangegeven in de beantwoording van vraag 45 actief met de aan te wijzen toezichthouders in gesprek om te bepalen wat de benodigde middelen zijn voor de uitvoering van het toezicht.

47

Is goed toezicht een harde randvoorwaarde om in te kunnen stemmen met de Omnibus Digitaal en de Omnibus AI?

Antwoord

Zoals altijd wordt het gehele pakket dat voorligt beoordeeld. De verordening schrijft voor dat de lidstaten voor voldoende middelen moeten zorgen om de toezichthouders in staat te stellen hun taak goed uit te voeren. Datzelfde geldt uiteraard ook voor de Commissie ten aanzien van het toezicht dat de AI Office uitoefent.

48

In het BNC-fiche lezen deze leden dat de regering de gevolgen voor de handhaafbaarheid onderzoekt, maar niet verwacht dat de voorstellen tot significante nieuwe uitdagingen met betrekking tot de uitvoering van de

onderliggende Europese wetten leidt omdat de voorstellen beogen de wetgeving te versimpelen.

In het BNC-fiche lezen deze leden verder: "Het voorstel zal implicaties hebben voor het toezicht op verschillende Europese regelgeving, dat nationaal is ingericht. Naar verwachting kunnen die taken worden ondergebracht bij de toezichthouders die nu al op deze Europese regelgeving toezien. Daarbij wordt gezocht naar de meest doeltreffende en doelmatige oplossing. Of de aanpassingen de kosten voor het toezicht en de handhaving zullen verhogen of verlagen is nog niet duidelijk. Het voorstel bevat ook enkele bepalingen die de AVG wijzigen en er mogelijk voor zullen zorgen dat er meer meldingen ontstaan bij de toezichthoudende autoriteit en de rechtspraak. Het kabinet verwacht niet dat er een omvangrijke verhoging in kosten van toezicht en handhaving zal zijn. Het versimpelen van de regels kan ook handhaving en toezicht vergemakkelijken. Het kabinet zal dit verder onderzoeken en opheldering vragen bij de Europese Commissie. De budgettaire gevolgen voor de Rijksbegroting worden ingepast op de begroting van de beleidsverantwoordelijke departementen, volgens de regels van de budgetdiscipline. Daarbij dient ook rekening gehouden te worden met medeoverheden".

Is dit nader onderzoek reeds afgerond? Zo ja, wat is daarvan de uitkomst?

Antwoord

Gezien de snelheid van de onderhandelingen is de inhoud van de omnibussen continu aan verandering onderhevig. Er kunnen dus nog geen definitieve conclusies worden getrokken over eventuele veranderingen in kosten voor toezicht en handhaving als gevolg van de omnibussen. Het kabinet verwacht nog steeds niet dat er als gevolg van de omnibussen een omvangrijke verhoging in kosten van toezicht en handhaving zal zijn. Het versimpelen van de regels kan ook handhaving en toezicht vergemakkelijken.

49

Hoe verhoudt de passage in het BNC-fiche zich tot de zorgen over de handhaafbaarheid vanuit de toezichthouders? Deze leden ontvangen graag een toelichting.

Antwoord

De primaire zorgen met betrekking tot handhaafbaarheid zien op enkele voorgestelde wijzigingen aan de AVG. Dat wordt gereflecteerd doordat wordt gesteld dat deze wijzigingen er mogelijk voor zullen zorgen dat er meer meldingen ontstaan bij de toezichthoudende autoriteit. Deze wijzigingen kunnen mogelijk leiden tot een toename van het aantal meldingen bij de toezichthouder.

50

Definitie persoonsgegevens en trainen AI-modellen

In het BNC-fiche lezen deze leden dat de regering ziet dat sommige aanpassingen aan de AVG een fundamentele impact hebben op het recht op privacy en het recht op gegevensbescherming, maar dat bij gebrek aan *impact assessment* en advies van de EPDB en EDPS de regering de proportionaliteit ervan niet kan beoordelen.

Inmiddels zijn, na het verschijnen van de BNC-fiches, de adviezen van de EDPS en het EDPB verschenen.

Hoe beoordeelt u deze adviezen?

Antwoord

In de gezamenlijke EDPB/EDPS-opinie over de Omnibus Digitaal zijn de EDPB en EDPS kritisch over de impact van de voorgestelde wijzigingen op het niveau van bescherming van de grondrechten op privacy en gegevensbescherming. De opinie komt op verschillende onderdelen overeen met het standpunt dat het kabinet ten aanzien van de Omnibus Digitaal en het kabinet ziet het dan ook als steun voor die positie.

51

Kunt u nogmaals reflecteren op de proportionaliteit van de aanpassingen aan de AVG na het lezen van de adviezen van de EDPB en EDPS?

Antwoord

In de gezamenlijke opinie van de EDPS/EDPB over de Digitale Omnibus wordt kritisch geoordeeld ten aanzien van de proportionaliteit van de aanpassingen aan de AVG. Bij gebrek aan impact assessments van de Commissie zelf, helpt dit om een oordeel te vellen over de evenredigheid van de voorstellen. Zoals is aangegeven in het BNC-fiche, is één van de voorgestelde wijzigingen aan de AVG die de meeste impact lijkt te hebben op het niveau van gegevensbescherming, de wijziging van de definitie van het begrip persoonsgegevens. Dit begrip bepaalt immers of de AVG – en alle rechten van betrokkenen – van toepassing is. Dat deze wijziging de meeste impact zou hebben, is inmiddels bevestigd in het advies van de EDPB en EDPS van 10 februari. Zij stellen dat deze wijziging zou leiden tot een aanzienlijke beperking in de reikwijdte van het begrip persoonsgegevens en aldus van de reikwijdte van de AVG. De EDPB en EDPS adviseren met kiem om de wijziging van deze definitie niet te aanvaarden. Hiervoor lijkt voldoende steun in de Raad. Ook op andere punten vindt het kabinet steun in de gezamenlijke opinie van de EDPS/EDPB, zoals onder meer het voorstel waarmee 'gerechtvaardigd belang' per definitie als grondslag lijkt te zijn gegeven voor het verwerken van persoonsgegevens voor het trainen en exploiteren van AI-systemen zonder dat daarvoor een noodzakelijkheidstoets en de bijbehorende belangenafweging noodzakelijk is. Andere voorbeelden zijn de kritische opmerkingen van de EDPB/EDPS over bijvoorbeeld de definitie van wetenschappelijk onderzoek, nieuwe bevoegdheden van de Europese Commissie tot uitvoeringshandelingen en de beperking van het inzagerecht.

52

Wat betekent dit voor het oordeel van de regering ten aanzien van de proportionaliteit van de Omnibus Digitaal en de Omnibus AI? Deze leden ontvangen graag een toelichting.

Antwoord

Zoals genoemd onder vraag 51, helpt de opinie bij het vormen van een oordeel over de proportionaliteit van de Omnibus Digitaal, zoals eerder ook de opinie over

de Omnibus AI heeft geholpen. Net als het kabinet, zijn de EDPB en de EDPS kritisch op verschillende voorstellen uit de Omnibus digitaal omdat deze afbreuk doen aan de bescherming van grondrechten, zonder dat ze effectief bijdragen aan het verlagen van regeldruk. Het kabinet ziet dit dan ook als steun voor die positie.

53

Het wijzigen van de definitie van persoonsgegevens in de Omnibus Digitaal heeft als voornaamste effect dat het trainen van AI-modellen makkelijker en juridisch toegankelijker wordt. De voorgestelde wijzigingen verkleinen de reikwijdte van wat als 'persoonsgegevens' wordt beschouwd, waardoor meer data gebruikt kan worden zonder expliciete toestemming van de betrokkenen. Het voorstel kent een aantal wijzigingen ten aanzien van de definitie en reikwijdte van persoonsgegevens, namelijk:

Nauwere definitie van persoonsgegevens: informatie die niet direct kan leiden tot identificatie van een persoon (bijvoorbeeld bepaalde gepseudonimiseerde data) wordt niet meer als 'persoonsgegeven' gezien als de ontvanger niet over de middelen beschikt om de persoon te identificeren. Dit maakt het eenvoudiger om grote datasets te gebruiken voor AI-training.

Wie is verantwoordelijk voor de beoordeling of de ontvanger niet over voldoende middelen beschikt om de persoon te identificeren; de afzender of de ontvanger? Wat betekent dit praktisch in de hele keten van informatie-uitwisseling?

Antwoord

Volgens de systematiek van de AVG is de verwerkingsverantwoordelijke verantwoordelijk voor de rechtmatige verwerking van persoonsgegevens en dient hij te kunnen aantonen dat hij aan de vereisten voldoet. Uitgaande van de voorgestelde wijziging, is er geen sprake van verwerking van persoonsgegevens door de ontvanger op het moment dat de ontvanger niet over voldoende middelen beschikt om de persoon te identificeren. Beschikt de ontvanger wel over die middelen, dan is er gewoon sprake van verwerking van persoonsgegevens en rusten er plichten op zowel de verzender als de ontvanger op grond van de AVG. Zowel de afzender als de ontvanger zijn dus verantwoordelijk voor deze beoordeling. Dit blijft zich herhalen in de keten van informatie-uitwisseling. De voorgestelde wijziging van het begrip persoonsgegevens zou het makkelijker maken voor schakels in ketens van informatie-uitwisseling om te beargumenteren dat gegevens vanuit hun perspectief gezien geen persoonsgegevens zijn.

54

Er is ook veel data die niet direct, maar indirect gegevens onthult. Bijvoorbeeld politieke voorkeur die afgeleid kan worden uit reacties en *likes* op een platform. Ook indirecte gegevens zoals locatiegegevens, surfgedrag, of aankoopgeschiedenis kunnen makkelijker worden gebruikt. Wat betekent deze aanpassing voor het beschermingsniveau? Deze leden ontvangen graag een toelichting.

Antwoord

Onder de voorgestelde wijziging blijven indirect identificerende gegevens onder de definitie van persoonsgegevens vallen. In dit opzicht is er dus geen wijziging. In het begin november jl. gelekte concept van het Commissievoorstel werd de reikwijdte van de definitie van bijzondere categorieën van persoonsgegevens weliswaar beperkt tot direct identificerende persoonsgegevens, waarmee indirect identificerende persoonsgegevens zouden worden uitgesloten. Deze wijziging is geen onderdeel van het officiële Commissievoorstel van 19 november jl.

55

De Autoriteit Persoonsgegevens (AP) waarschuwt voor het risico op grootschalige surveillance als indirecte identificatie niet meer onder de AVG valt. Het wordt makkelijker om op basis van "anonieme" data profielen te maken die in de praktijk alsnog naar individuen herleidbaar zijn, wat kan leiden tot ongewenste monitoring. Hoe oordeelt u over dit risico? Deze leden ontvangen graag een toelichting.

Antwoord

Zoals aangegeven in de beantwoording van vraag 54 blijven onder de voorgestelde wijziging indirect identificerende gegevens onder de definitie van persoonsgegevens vallen.

56

De EDPB en EDPS waarschuwen dat de 'versmalling' van de definitie van persoonsgegevens een juridisch gat creëert: als data niet langer als 'persoonlijk' wordt gezien, vervallen alle AVG-waarborgen automatisch, waardoor de nieuwe 'extra' regels weinig effect hebben. Hoe oordeelt u over dit risico?

Antwoord

Het kabinet deelt de analyse van de EDPB en EDPS dat versmalling van de definitie van persoonsgegevens er in specifieke gevallen toe kan leiden dat data niet langer als persoonsgegevens kunnen worden gezien, wat zou betekenen dat de AVG niet van toepassing is.

57

Hoe oordeelt u over deze aanpassing als geheel?

Antwoord

Het kabinet ziet dat deze nieuw voorgestelde definitie vragen oproept en dat de gevolgen hiervan niet direct duidelijk zijn. Volgens de Commissie zou de wijziging een codificatie van het SRB-arrest betreffen, maar op basis van de eerste analyse van het kabinet gaat het voorstel verder dan een codificatie.²¹ Het voorstel lijkt namelijk een wijziging aan te brengen ten opzichte van een overweging van het Hof van Justitie van de Europese Unie over de vraag of gepseudonimiseerde gegevens ook in meerdere schakels van een keten als persoonsgegevens moeten

²¹ Zie onder meer J. Mannekens, annotatie bij HvJ EU 4 september 2025 (SRB-arrest), nr. C-413/23 P, Computerrecht 2025/195 en I. Ezzamouri en R.P. Santifort, annotatie bij diezelfde uitspraak, *Jurisprudentie Bescherming Persoonsgegevens* 2025, blz. 1135-1138,

worden beschouwd.²² Sommige elementen uit de jurisprudentie lijken in de voorgestelde definitie te ontbreken, zoals het feit dat de specifieke entiteit die de gegevens verwerkt, via derde partijen toegang kan verkrijgen tot identificatiemiddelen, ook een relevant criterium is voor de vraag of sprake is van persoonsgegevens (voor die entiteit).²³ In Nederlandse rechtspraak wordt dit criterium zo uitgelegd dat bepalend is welke middelen de ontvanger feitelijk ter beschikking heeft om gegevens te herleiden tot individuen.²⁴

Verder noemt de voorgestelde definitie niet het criterium of de ontvanger in staat is de pseudonimisering ongedaan te maken.²⁵ Het kabinet heeft de Commissie daarom gevraagd de door haar voorgestelde wijzigingen te verduidelijken, nader toe te lichten en de effecten te beoordelen.

De EDPB en EDPS waarschuwen in hun advies van 10 februari jl. uitdrukkelijk voor de voorgestelde wijzigingen in de definitie van persoonsgegevens, aangezien deze wijzigingen veel verder gaan dan een gerichte of technische wijziging van de AVG. Bovendien weerspiegelen de voorstellen volgens de EDPB en EDPS niet nauwkeurig de jurisprudentie en gaan zij duidelijk verder en zouden zij leiden tot een aanzienlijke beperking in de reikwijdte van het begrip persoonsgegeven, en aldus van de reikwijdte van de AVG. De door de Commissie gedane voorstel tot wijziging van het begrip persoonsgegevens, zou rechtsonzekerheid over het toepassingsbereik van de AVG bij organisaties in de hand kunnen werken. Meerdere lidstaten lijken kritisch te zijn op de door de Commissie voorgestelde wijzigingen van het begrip persoonsgegevens.

58

Wat betekent deze aanpassing voor het toezicht? Welke (mogelijke) knelpunten worden hierbij voorzien?

Antwoord

Als de definitie van persoonsgegevens zoals voorgesteld door de Commissie zou worden aangepast, zouden bedrijven sneller aannemelijk kunnen maken dat (vanuit hun perspectief) geen persoonsgegevens worden verwerkt. Voor betrokkenen zou het moeilijker kunnen worden om te beoordelen of die stelling juist is, wat zou kunnen leiden tot meer klachten bij toezichthouders. Ook zou de aanpassing ertoe kunnen leiden dat het voor toezichthouders lastiger wordt om te bepalen of zij bevoegd zijn. De AP heeft in haar position paper van 13 januari jl. gesignaleerd dat toezichthouders door de voorgestelde aanpassing van de definitie van persoonsgegevens minder zicht op risico's hebben, dat de bescherming van

²² HvJ EU 04-09-2025, C-413/23 P, ECLI:EU:C:2025:645, paragraaf 85: "Voor zover niet is uitgesloten dat deze derden redelijkerwijs in staat zullen zijn om met middelen, zoals een vergelijking met andere gegevens waarover zij beschikken, de gepseudonimiseerde gegevens te koppelen aan de betrokkene, moet deze persoon dus worden geacht identificeerbaar te zijn, zowel wat de doorgifte als wat de verdere verwerking van die gegevens door die derden betreft.

²³ Hof van Justitie EU 7 maart 2024, C-604/22, ECLI:EU:C:2024:214 (IAB Europe/Gegevensbeschermingsautoriteit), paragraaf 46, en HvJEU 7 maart 2024, C-479/22, ECLI:EU:C:2024:215 (OC/Europese Commissie), paragraaf 55.

²⁴ Rb. Midden-Nederland 23 april 2025, ECLI:NL:RBMNE:2025:1760, rechtsoverweging 3.10 – 3.13.

²⁵ HvJ EU 04-09-2025, C-413/23 P, ECLI:EU:C:2025:645, paragraaf 77.

sommige (gepseudonimiseerde) persoonsgegevens in het geding komt en dat mensen daardoor minder goed beschermd zijn.²⁶

59

Wat betekent deze aanpassing voor de (grond)rechten/positie van burgers/consumenten? Deze leden ontvangen graag een toelichting.

Antwoord

Zoals aangegeven in de beantwoording van vragen 57 en 58 zou de voorgestelde wijziging afbreuk doen aan het niveau van bescherming van persoonsgegevens.

60

Past deze aanpassing in de actuele strategie om minder afhankelijk te worden van de grote (Amerikaanse) techbedrijven? Deze leden ontvangen graag een toelichting.

Antwoord

Deze voorgestelde aanpassing is niet direct relevant voor het versterken van de digitale open strategische autonomie, maar zou wel de rechtspositie van burgers in relatie tot techbedrijven kunnen verzwakken. Als de voorgestelde wijziging van de definitie van persoonsgegevens zou worden doorgezet, zou de AVG minder vaak van toepassing zijn. Dat zou dan ook bijvoorbeeld gelden voor de mogelijkheden die de AVG aan betrokkenen biedt om hun privacyrechten uit te oefenen jegens (tech)bedrijven, of voor de bevoegdheden van toezichthouders. Zoals de EDPB en EDPS hebben opgemerkt in hun gezamenlijke opinie, maakt een beperking van de definitie van persoonsgegevens het moeilijker voor betrokkenen om hun rechten uit te oefenen..

61

Ruimere interpretatie van 'legitiem belang': het trainen van AI-modellen en het doen van wetenschappelijk onderzoek worden expliciet erkend als legitieme belangen onder de AVG. Hierdoor is geen toestemming nodig, mits er passende waarborgen zijn. De Omnibus Digitaal erkent expliciet dat onderzoek door commerciële partijen, zoals het trainen van AI-modellen door een techbedrijf, als wetenschappelijk onderzoek kan worden aangemerkt, mits het bijdraagt aan de algemene stand van de techniek en wetenschap.

Hoe oordeelt u over de voorgestelde waarborgen?

Antwoord

Het kabinet deelt de opvatting dat een te ruime definitie van wetenschappelijk onderzoek in de AVG – waarbij expliciet ook onderzoek voor commerciële doeleinden is inbegrepen – afbreuk kan doen aan het beschermingsniveau onder de AVG. De voorgestelde definitie is uiterst breed en wijkt af van de definities van de EDPB (richtsnoeren 05/2020) en EDPS (opinie 6 januari 2020). Het kabinet is

²⁶ <https://www.autoriteitpersoonsgegevens.nl/documenten/position-paper-ap-omnibus-digitaal-en-omnibus-ai>

bezorgd dat de voorgestelde definitie van wetenschappelijk onderzoek, vormen van onderzoek omvat die niet wetenschappelijk zijn. Het kabinet is dan ook bezorgd dat de voorgestelde definitie afbreuk kan doen aan de bescherming op basis van de AVG. De AVG biedt bij wetenschappelijk onderzoek immers o.a. uitzonderingen op de rechten van betrokkenen (artikel 89, tweede lid), zoals de uitzonderingen op de informatieplicht, het recht op gegevenswissing en op rectificatie. Het kabinet heeft voorgesteld om de definitie van wetenschappelijk onderzoek te schrappen, of te behandelen op een manier die recht doet aan de zorgen over en potentiële impact van deze wijziging. Verschillende lidstaten lijken het schrappen van de definitie te steunen.

62

Hoe oordeelt u over deze aanpassing als geheel?

Antwoord

Zoals ook in het BNC-fiche is benadrukt, heeft het kabinet bij een aantal fundamentele wijzigingen aan de AVG serieuze zorgen, omdat deze wijzigingen het niveau van gegevensbescherming wezenlijk verminderen, zonder dat er sprake is van een effectieve bijdrage aan het verlagen van regeldruk.

Op dit moment kan het verwerken van persoonsgegevens voor AI-doeleinden toegestaan zijn, zoals ook volgt uit EDPB Advies 28/2024 over bepaalde aspecten van gegevensbescherming in verband met de verwerking van persoonsgegevens in het kader van AI-modellen. De verwerkingsverantwoordelijke moet hierbij wel aan verschillende voorwaarden voldoen. De EDPB en EDPS hebben dit in hun advies van 10 februari 2026 bevestigd, en aangegeven dat het daarom niet nodig is om hierover een specifieke bepaling op te nemen in de AVG.

In het BNC-fiche is benoemd dat het voorstel lijkt vast te leggen dat bij de training en exploitatie van een AI-model de grondslag 'gerechtvaardigd belang' per definitie is gegeven zonder dat een noodzakelijkheidstoets en de bijbehorende belangenafweging moet plaatsvinden. Het voorstel voorziet ook in de verwerking van bijzondere persoonsgegevens voor dit doel (artikel 9, tweede lid, onder k, en vijfde lid, AVG). Juist vanwege de gevolgen die de verwerking van deze bijzondere categorieën van persoonsgegevens voor de betrokkenen kunnen hebben, genieten zij extra bescherming. Wanneer deze persoonsgegevens ook mogen worden verwerkt voor genoemd doel, is het extra belangrijk dat er goede randvoorwaarden zijn. Of deze mogelijkheden verder moeten worden verruimd, vergt nadere beoordeling. Verdere verruiming zou alleen aan de orde kunnen zijn als de fundamentele rechten voldoende gewaarborgd zijn. Hierop wordt nader ingegaan in het antwoord op vraag 10 van de Volt-fractie.

63

Wat betekent deze aanpassing voor het toezicht? Welke (mogelijke) knelpunten worden hierbij voorzien?

Antwoord

De AP heeft in haar position paper aangegeven dat het voorgestelde artikel 88c juist minder duidelijkheid creëert. Op dit moment wordt de grondslag van een

gerechtvaardigd belang in AI-context niet uitgesloten, maar de aanbieders of ontwikkelaars moeten altijd nagaan of het de meest geschikte grondslag is en een belangenafweging maken. De AP stelt: "Deze bepaling suggereert een verruiming die er niet is. In andere woorden: deze wijziging is overbodig en creëert alleen meer verwarring." Dit zou ook kunnen doorwerken in het toezicht: situaties waarvoor de toezichthoudende autoriteiten reeds richtsnoeren hadden vastgesteld zouden opnieuw moeten worden beoordeeld op grond van artikel 88c.

64

Wat betekent deze aanpassing voor de (grond)rechten/positie van burgers/consumenten? Deze leden ontvangen graag een toelichting.

Antwoord

Op dit moment moeten verwerkingsverantwoordelijken volgens de AVG een belangenafweging maken tussen hun eigen belangen en de rechten van de betrokkene, om te bepalen of de grondslag inzake een gerechtvaardigd belang passend is. In EDPB Advies 28/2024 is bevestigd dat er een gerechtvaardigd belang kan zijn, maar dat dit een specifieke belangenafweging vergt. Door in de AVG op te nemen dat verwerking van persoonsgegevens in het kader van de ontwikkeling en exploitatie van een AI-systeem of AI-model een gerechtvaardigd belang kan vormen, zou de Europese wetgever hieraan een zwaar gewicht geven omdat de AVG momenteel nog nergens anders een precedent kent van een bepaling waarin staat dat een specifieke gegevensverwerking of toepassing kan leiden tot een gerechtvaardigd belang.

Dit voorstel zou daarmee zo kunnen worden opgevat dat de ontwikkeling en exploitatie van AI in principe als een gerechtvaardigd belang moet worden beschouwd. Dit zou het mogelijk ook voor betrokkenen moeilijker kunnen maken om te betwisten dat er een gerechtvaardigd belang is. Zoals in het BNC-fiche is opgemerkt, zou de expliciete vermelding van de grondslag 'gerechtvaardigd belang' de indruk kunnen wekken dat deze rechtsgrondslag per definitie is gegeven zonder dat een noodzakelijkheidstoets en de bijbehorende belangenafweging moet plaatsvinden. De AP geeft in haar position paper van 13 januari jl. terecht aan dat de bepaling een verruiming suggereert die er niet is.²⁷ Dit zou ertoe kunnen leiden dat AI-bedrijven vaker stellen dat hun activiteiten onder een gerechtvaardigd belang vallen en dat zij dus geen toestemming hoeven te vragen. Concreet zou dit kunnen betekenen dat berichten, foto's of spraakopnamen van betrokkenen vaker worden gebruikt om AI-systemen te trainen zonder toestemming van betrokkenen. Weliswaar kunnen betrokkenen hiertegen bezwaar maken (opt-out), maar het risico bestaat dat betrokkenen vaak niet weten wanneer of door wie hun gegevens worden gebruikt voor AI-trainingsdoeleinden, of dat zij bij een in potentie groot aantal bedrijven bezwaar zouden moeten maken om verwerking van hun persoonsgegevens te voorkomen. Hierop wordt nader ingegaan in het antwoord op vraag 95. Een verslechtering van de rechtspositie van betrokkenen lijkt temeer een risico omdat in artikel 88c belangrijke voorwaarden ontbreken die de EDPB wel heeft

²⁷ <https://www.autoriteitpersoonsgegevens.nl/documenten/position-paper-ap-omnibus-digitaal-en-omnibus-ai>

genoemd in Advies 28/2024. Zo ontbreekt de voorwaarde dat rekening moet worden gehouden met de redelijke verwachtingen van de betrokkene, waarbij onder meer rekening moet worden gehouden met de vraag of de persoonsgegevens al openbaar waren en of er een relatie bestaat tussen de betrokkene en de verwerkingsverantwoordelijke. Bovendien roept het artikel, hoewel het de bedoeling is de huidige AVG-regels te verduidelijken, nieuwe vragen op. Bijvoorbeeld met betrekking tot het "onvoorwaardelijke recht van bezwaar" en de relatie van het artikel tot het advies 28/2024 van het EDPB.

65

Onder andere European Digital Rights (EDRI), een koepelorganisatie van burgerrechtenorganisaties, waarschuwt dat de Omnibus Digitaal een "vrijbrief" geeft aan grote (Amerikaanse) techbedrijven om de AVG te omzeilen door middel van een vage definitie over "wetenschappelijk onderzoek" en "gerechtvaardigd belang" bij het trainen van AI.²⁸

Kunt u reflecteren op deze waarschuwing? Deze leden ontvangen graag een toelichting.

Antwoord

Hiervoor verwijs ik u naar de beantwoording van vraag 61 en vraag 64.

66

Deelt u de opvatting dat het legitimeren van dataverzameling voor het trainen van AI-systemen zonder toestemming uitsluitend de machtspositie van grote spelers zal versterken, die reeds over gigantisch veel data beschikken, en dat dit schadelijk is voor privacy van EU-burgers en eerlijke concurrentie met Europese bedrijven?

Antwoord

Zoals toegelicht in het antwoord op vraag 64 kan de verwerking van persoonsgegevens op dit moment onder bepaalde voorwaarden op grond van de grondslag "gerechtvaardigd belang" plaatsvinden. Dit vergt echter een belangenafweging, aldus advies 28/2024 van het EDPB. Het voorgestelde artikel 88c zou het voor betrokkenen moeilijker kunnen maken om te betwisten dat er een gerechtvaardigd belang is. In zoverre bestaat het risico dat deze aanpassing meer ten goede komt aan bestaande AI-bedrijven die al beschikken over datasets, inclusief persoonsgegevens, en daardoor voor hun werkwijze makkelijker een legitimatie kunnen vinden door een specifieke AVG-bepaling dan (beginnende) AI-bedrijven die geen datasets met persoonsgegevens hebben en die niet voornemens zijn om persoonsgegevens te gebruiken (zonder toestemming van betrokkenen).

67

²⁸ EDRI, 'Why the Digital Omnibus puts GDPR and ePrivacy at risk', 202511-Eexplaining-GDPR_eprivacy-Digital-Omnibus.pdf.

Past deze aanpassing in de actuele strategie om minder afhankelijk te worden van de grote (Amerikaanse) techbedrijven? Deze leden ontvangen graag een toelichting.

Antwoord

Deze voorgestelde aanpassing is niet direct relevant voor het versterken van de digitale open strategie autonomie. Zoals toegelicht in antwoord 66, bestaat wel het risico dat deze aanpassing meer ten goede komt aan bestaande AI-bedrijven die al beschikken over datasets, inclusief persoonsgegevens, en daardoor voor hun werkwijze makkelijker een legitimatie kunnen vinden door een specifieke AVG-bepaling.

68

Gebruik van gevoelige data voor bias-detectie: het gebruik van bijzondere persoonsgegevens over bijvoorbeeld etniciteit, religie of gezondheid, voor het opsporen en corrigeren van bias in AI-systemen wordt verruimd. Zo wordt de doelgroep voor het gebruik van data voor bias-detectie verruimd: waar de AI-verordening deze uitzondering momenteel beperkt tot aanbieders van hoog-risico systemen, breidt de Omnibus AI dit uit naar aanbieders én gebruikers van alle AI-systemen en -modellen.

Hoe oordeelt u over deze aanpassing?

Antwoord

De verwerking van bijzondere categorieën van persoonsgegevens is in beginsel verboden en kan alleen onder specifieke voorwaarden worden toegestaan, omdat de context van de verwerking ervan significante risico's kan meebrengen voor de grondrechten en fundamentele vrijheden (overweging 51 AVG). Het is in dat licht niet wenselijk om ambigue of ruime uitzonderingen te maken voor de verwerking van bijzondere categorieën van persoonsgegevens. Een strikte limitering tot verwerking voor bias-detectie en -correctie is wenselijk.

Dit is ook benadrukt in de Opinie van het EDPB en de EDPS. De EDPB en de EDPS vinden dat een dergelijke gegevensverwerking alleen dient te zijn toegestaan in strikt afgebakende situaties, wanneer het risico op discriminatie ernstig is en er passende waarborgen gelden. EDPB en EDPS adviseren om de eis te behouden die nu al geldt op grond van artikel 10, tweede lid, onder f, en vijfde lid, aanhef, namelijk dat de gegevensverwerking strikt noodzakelijk is voor de beoordeling en correctie met het oog op mogelijke vooringenomenheid die waarschijnlijk gevolgen heeft voor de gezondheid en de veiligheid van personen, nadelige effecten heeft op de grondrechten, of leidt tot discriminatie die op grond van het Unierecht verboden is, vooral wanneer data-outputs invloed hebben op inputs voor toekomstige operaties.

Het kabinet zet erop in het voorstel op dit punt in lijn te brengen met de opinie van de EDPB en EDPS. Wanneer het kabinet uitsluitend kan geven of de waarborgen in het voorstel voldoende proportioneel zijn hangt af van het verloop van de onderhandelingen. Er lijkt voldoende steun in de Raad om de voorwaarden

waaronder bijzondere categorieën van persoonsgegevens mogen worden verwerkt voor biasdetectie en -correctie aan te scherpen.

69

Wat betekent deze aanpassing voor het toezicht? Welke (mogelijke) knelpunten worden hierbij voorzien?

Antwoord

Deze aanpassing zou betekenen dat waar toezichthouders voorheen alleen toezicht moesten houden op het gebruik van deze mogelijkheid binnen de context van hoog risico AI-systemen, dit nu ook zouden moeten doen in de context van alle AI-systemen. Voor wat betreft de voorgestelde aanpassing van het artikel zijn geen (significante) gevolgen voor het toezicht voorzien.

70

Wat betekent deze aanpassing voor de (grond)rechten/positie van burgers/consumenten? Deze leden ontvangen graag een toelichting.

Antwoord

Eenzijds leidt deze aanpassing tot een mogelijke verbetering van het recht op non-discriminatie, omdat er meer AI-systemen aan een grondigere bias-controle en -correctie onderworpen kunnen worden. Anderzijds kan verkeerd gebruik van deze mogelijkheid leiden tot inbreuken op het recht op gegevensbescherming. Daarom pleit het kabinet tijdens de onderhandelingen voor duidelijke waarborgen en een strikte noodzakelijkheid.

71

Organisaties mogen biometrische gegevens verwerken wanneer het noodzakelijk is om de identiteit van een betrokkene te verifiëren en de gegevens en middelen voor deze verificatie onder de uitsluitende controle van de betrokkene zijn.

Wat betekent precies "onder uitsluitende controle van betrokkenen zijn" in de situatie waarbij een werkgever dit wil gebruiken voor de toegangscontrole van medewerkers?

Antwoord

Het voorgestelde artikel 9(2)(l) AVG is van toepassing wanneer de biometrische gegevens of de middelen die nodig zijn voor de verificatie onder de exclusieve controle van de betrokkene vallen. Dit betekent dat de verwerkingsverantwoordelijke geen kennis krijgt van de biometrische gegevens of slechts gedurende een zeer beperkte tijd. Indien de betrokkene niet daadwerkelijk de exclusieve controle over het verificatieproces heeft, is de bepaling niet van toepassing en kan er geen beroep worden gedaan op de uitzondering.

72

De EDPB en EDPS uiten kritiek op het feit dat de Omnibus AI voorziet in een wijziging van de grondslag voor de verwerking van bijzondere persoonsgegevens, waarbij de eis van "strikt noodzakelijk" wordt vervangen door de minder strenge eis van "noodzakelijk".

Hoe oordeelt u over deze specifieke aanpassing?

Antwoord

Het kabinet deelt deze kritiek. Daarom pleit het kabinet tijdens de onderhandelingen voor strikte noodzakelijkheid. Binnen de Raad lijken meerdere lidstaten dit te steunen.

73

Wat betekent deze aanpassing voor het toezicht? Welke (mogelijke) knelpunten worden hierbij voorzien?

Antwoord

Hiervoor verwijs ik u naar het antwoord op vraag 69.

74

Wat betekent deze aanpassing voor de (grond)rechten/positie van burgers/consumenten? Deze leden ontvangen graag een toelichting.

Antwoord

Hiervoor verwijs ik u naar het antwoord op vraag 70.

75

De Europese Commissie stelt enkele waarborgen voor, namelijk:

- **Strikte doelbinding:** De verwerking van gegevens over gezondheid, religie of etniciteit is alleen toegestaan voor het detecteren en corrigeren van bias. Zodra de bias is verholpen, moet de data in principe worden verwijderd of geanonimiseerd.
- **Beperkte toegang:** Alleen geautoriseerd personeel mag met deze gevoelige datasets werken. Er moeten technische barrières zijn (zoals 'clean rooms' of beveiligde omgevingen) om te voorkomen dat de data weglekt naar andere afdelingen.
- **Transparantie en documentatie:** Ontwikkelaars moeten in hun technische documentatie vastleggen waarom het gebruik van deze data noodzakelijk was en welke maatregelen zijn genomen om de privacy te beschermen.
- **Toezicht door het AI-bureau:** Dit nieuwe Europese orgaan moet toezien op de naleving van deze regels bij de machtigste AI-modellen.

Hoe oordeelt u over deze waarborgen?

Antwoord

Het kabinet is positief over deze waarborgen. Onder andere deze en andere waarborgen staan al in de AI-verordening en zijn dus ook al van toepassing op de bestaande grondslag voor hoog risico AI-systemen. Het kabinet heeft deze tijdens de onderhandelingen over de AI-verordening gesteund. Naast deze waarborgen pleit het kabinet voor het behouden van strikte noodzakelijkheid.

76

Wat betekent deze aanpassing voor het toezicht? Welke (mogelijke) knelpunten worden hierbij voorzien?

Antwoord

Hiervoor verwijs ik u naar het antwoord op vraag 69.

77

Wat betekent deze aanpassing voor de (grond)rechten/positie van burgers/consumenten? Deze leden ontvangen graag een toelichting.

Antwoord

Hiervoor verwijs ik u naar het antwoord op vraag 70.

78

Nationale toezichthouders en de EDPB en EDPS waarschuwen voor:

- Het risico op *'function creep'*. Dit behelst het risico dat de data die verzameld worden voor bias-correctie in de praktijk voor andere (commerciële) doeleinden gebruikt kunnen worden zodra de drempel voor verwerking is verlaagd;
- Nieuwe vormen van profilering. Hoewel het doel "eerlijkheid" is, kunnen bedrijven deze gevoelige data indirect gebruiken om gedrag te voorspellen. Zo kan een verzekeraar of bank AI-modellen bouwen die patronen herkennen die samenhangen met religie of gezondheid, wat kan leiden tot uitsluiting op basis van statistische profielen.
- Inbreuk op de private sfeer. Gegevens over religie en etniciteit behoren tot de meest persoonlijke informatie. Critici vrezen dat het "normaliseren" van het gebruik hiervan in AI-training de psychologische drempel verlaagt voor overheden en bedrijven om deze data op grote schaal te monitoren.

Hoe oordeelt u over deze voorziene risico's?

Antwoord

Dit zijn inderdaad mogelijke risico's bij het verruimen van de mogelijkheid om bijzondere categorieën van persoonsgegevens te verwerken voor bias-controle- en correctie. Daarom pleit het kabinet voor strikte waarborgen om deze risico's te beperken.

79

Wat betekent dit voor het toezicht? Welke (mogelijke) knelpunten worden hierbij voorzien?

Antwoord

Hiervoor verwijs ik u naar het antwoord op vraag 69.

80

Wat betekent dit de (grond)rechten/positie van burgers/consumenten? Deze leden ontvangen graag een toelichting.

Antwoord

Hiervoor verwijs ik u naar het antwoord op vraag 70.

81

De EDPB en EDPS vinden dat gebruik van gevoelige gegevens voor bias-detectie alleen zou mogen in strikt afgebakende situaties, bijvoorbeeld wanneer de risico's van discriminatie ernstig zijn en er passende waarborgen gelden. De EDPB en EDPS adviseren om het gebruik van gevoelige gegevens (zoals etniciteit of gezondheidsdata) voor bias-detectie expliciet te beperken tot gevallen waarin het risico op ernstige nadelige gevolgen door bias aangetoond kan worden.

Kunt u reflecteren op dit advies? Onderschrijft u deze voorwaarde?

Antwoord

Zoals aangegeven in het antwoord op vraag 68 zet het kabinet erop in het voorstel op dit punt in lijn te brengen met de opinie van de EDPB en EDPS.

82

Is aanpassing van dit onderdeel een harde randvoorwaarde om in te kunnen stemmen met de Omnibus AI?

Antwoord

Het kabinet pleit in ieder geval nadrukkelijk voor het behouden van de strikte noodzakelijkheid. Het kabinet zal de uiteindelijke Omnibus AI in zijn geheel wegen en op basis daarvan bepalen of zij met de Omnibus AI kan instemmen.

83

De EDPB en EDPS benadrukken dat nationale gegevensbeschermingsautoriteiten in de eerste plaats bevoegd zouden moeten zijn om toezicht te houden op de verwerking van persoonsgegevens.

Hoe oordeelt u over dit advies? Onderschrijft u deze voorwaarde?

Antwoord

In punt 16 uit het advies van EDPB/EDPS over de Omnibus AI benadrukken de EDPB en EDPS dat de gegevensbeschermingsautoriteiten in de eerste plaats bevoegd zijn om toezicht te houden op de verwerking van persoonsgegevens op grond van artikel 4a van de AI-wetgeving, ook in overeenstemming met artikel 2, lid 7, van de AI-wetgeving. Ik beschouw dit niet zozeer als een advies, maar als een (logische) constatering.

84

Is aanpassing van dit onderdeel een harde randvoorwaarde om in te kunnen stemmen met de Omnibus AI?

Antwoord

Het kabinet zal de uiteindelijke Omnibus AI in zijn geheel wegen en op basis daarvan bepalen of zij met de Omnibus AI kan instemmen.

85

In het kader van de proportionaliteitsbeoordeling lezen de leden van de fractie GroenLinks-PvdA in het BNC-fiche dat de regering vraagtekens heeft over de proportionaliteit van de voorstellen ten aanzien van de gegevensbescherming in relatie tot de vermindering van de regeldruk: *"Sommige wijzigingen aan de AVG lijken verder te gaan dan noodzakelijk omdat de wijzigingen afbreuk doen aan respectievelijk gegevensbescherming en onvoldoende duidelijk is in hoeverre deze voorstellen effectief regeldruk verlagen. Het kabinet zal opheldering vragen bij de Commissie en de gevolgen voor regeldruk, uitvoerbaarheid en bescherming van grondrechten verder in kaart te brengen voordat het tot een definitief oordeel komt op deze onderdelen. Het kabinet hecht eraan dat er in het bijzonder voor wijzigingen met impact op gegevensbescherming en fundamentele rechten gelegenheid is om de voorstellen en de gevolgen daarvan gedegen te analyseren en deze inhoudelijk te bespreken".*

Is er inmiddels meer helderheid over de geconstateerde onduidelijkheden?

Antwoord

Voor wat betreft het verzoek om een formeel impact assessment verwijs ik u naar de beantwoording van vragen 1 tot en met 3. In aanvulling hierop merk ik op dat, zoals in deze beantwoording toegelicht ten aanzien van specifieke artikelen, er voldoende steun in de Raad lijkt om een aantal bepalingen uit het voorstel te schrappen of aan te passen. De onderhandelingen zijn echter nog in volle gang. Ik zal u conform de informatie-afspraken informeren over het verdere verloop van de onderhandelingen.

86

Is een nader oordeel over de proportionaliteit van dit onderdeel?

Antwoord

Voor beoordelingen van de voorgestelde aanpassingen aan de AVG verwijs ik u naar de beantwoording van vragen 57, 61, 62, 68 en 85.

87

Past deze aanpassing in de actuele strategie om minder afhankelijk te worden van de grote (Amerikaanse) techbedrijven? Deze leden ontvangen graag een toelichting.

Antwoord

Deze voorgestelde aanpassing is niet direct relevant voor het versterken van de digitale open strategische autonomie, maar zoals aangegeven in het antwoord op vragen 60 en 67 kunnen sommige van deze voorgestelde wijzigingen wel de rechtspositie van burgers in relatie tot techbedrijven verzwakken of bedrijven die al toegang tot veel data hebben meer bevoordelen.

88

Geautomatiseerde besluitvorming

De leden van de fractie van GroenLinks-PvdA merken op dat artikel 22 van de AVG fundamenteel wordt herzien. Op dit moment heeft een betrokkene het recht om niet onderworpen te worden aan geautomatiseerde besluitvorming zonder

menselijke tussenkomst als dat een rechtsgevolg of ander gevolg heeft dat hem of haar significant raakt. Daar zijn een aantal uitzonderingen op. Deze negatieve formulering 'mag niet, behalve' wordt in het voorstel omgedraaid naar een positieve formulering: het mag als er aan bepaalde voorwaarden wordt voldaan.

Hoe oordeelt u over deze aanpassing?

Antwoord

De voorgestelde wijziging van artikel 22 AVG, over verwerking van persoonsgegevens voor geautomatiseerde individuele besluitvorming, wijzigt de formulering van dit artikel zo dat het recht van de betrokkene verandert in een verplichting voor de verwerkingsverantwoordelijke. Deze gewijzigde formulering zou geen verandering van de rechten van betrokkenen mogen inhouden. Nederland heeft daarom voorgesteld om in de bijbehorende overweging 38 te expliciteren dat de voorgestelde wijzigingen de rechten van betrokkenen niet veranderen. De EDPB en EDPS hebben in hun advies van 10 februari 2026 een alternatieve formulering voorgesteld,²⁹ die blijft uitgaan van een verbod met uitzonderingen (nee-tenzij regel), om te voorkomen dat de mogelijkheden voor geautomatiseerde individuele besluitvorming te breed worden geïnterpreteerd. Op die manier zou duidelijk zijn dat er geen sprake is van een materiële verandering, wat zou aansluiten bij het oogmerk van het Nederlandse voorstel.

De voorgestelde wijziging van artikel 22 AVG heeft daarnaast betrekking op de beoordeling of een besluit noodzakelijk is voor het sluiten of uitvoeren van een overeenkomst tussen de betrokkene en een verwerkingsverantwoordelijke. Het voorstel verduidelijkt dat niet mag worden vereist dat het besluit uitsluitend door middel van geautomatiseerde verwerking kan worden genomen. In overweging 38 wordt aangegeven 'dat het feit dat het besluit ook door een mens kan worden genomen, de verwerkingsverantwoordelijke er niet van weerhoudt het besluit te nemen door uitsluitend geautomatiseerde verwerking'. In 1.2.2.7 van het SWD geeft de Europese Commissie aan dat de huidige formulering ruimte laat voor een (ongewenst geachte) restrictieve interpretatie die het gebruik van geautomatiseerde tools belemmert, bijvoorbeeld op het gebied van cyberbeveiliging en fraudepreventie, of in de precontractuele fase.

De EDPB en EDPS hebben in hun advies van 10 februari jl. geadviseerd om het voorgestelde artikel 22, eerste lid, onder a, over te hevelen naar overweging 38, en anders te verwoorden, om te verduidelijken dat de algemene eisen van noodzakelijkheid en dataminimalisatie uit artikel 5 en 6(1)(b) AVG onverkort gelden. Ook adviseren zij om in overweging 38 te verduidelijken dat geautomatiseerde individuele besluitvorming alleen noodzakelijk is als de verwerkingsverantwoordelijke niet beschikt over andere even effectieve en minder ingrijpende middelen (al dan niet geautomatiseerd). Het kabinet bestudeert dit advies momenteel nader, maar ook het kabinet is ervan uitgegaan dat een dergelijke beoordeling ook in de toekomst vereist blijft, omdat die rechtstreeks

²⁹ Zie §66 van het advies: "a decision which produces legal effects for a data subject or similarly significantly affects them shall not be based solely on automated processing, including profiling, unless that decision: (...)"."

voortvloeit uit de algemene vereisten van noodzakelijkheid, subsidiariteit en proportionaliteit die bij artikel 5, 6 en 22 AVG van toepassing zijn.

89

Wat betekent dit voor het toezicht? Welke mogelijke knelpunten worden hierbij voorzien?

Antwoord

Voor wat betreft de voorgestelde aanpassingen van artikel 22 zijn geen (significante) gevolgen voor het toezicht voorzien.

90

Wat betekent dit de (grond)rechten/positie van burgers/consumenten? Deze leden ontvangen graag een toelichting.

Antwoord

Hiervoor verwijs ik u naar het antwoord op vraag 88.

91

Past deze aanpassing in de actuele strategie om minder afhankelijk te worden van de grote (Amerikaanse) techbedrijven? Deze leden ontvangen graag een toelichting.

Antwoord

Deze voorgestelde aanpassing is niet direct relevant voor het versterken van de digitale open strategische autonomie.

92

Effecten gecentraliseerde toestemming voor het Nederlandse en Europese medialandschap

De leden van de fractie van GroenLinks-PvdA lezen in een position paper van NDP Nieuwsmedia, een branchevereniging voor nieuwsmedia, dat zij bezorgd zijn over de aangekondigde Omnibus Digitaal. De Omnibus Digitaal grijpt volgens NDP Nieuwsmedia op onwenselijke wijze in op Nederlandse nieuwsmedia en brengt daarmee het behoud van een vitaal Nederlands journalistiek landschap in gevaar, omdat steeds meer advertentie-inkomsten richting Big-Tech vloeien. Juist in een tijd waarin grote (Amerikaanse) techbedrijven steeds meer invloed krijgen op de informatievoorziening, is het behoud van een vitaal journalistiek landschap van groot maatschappelijk belang.

Deze leden lezen dat de Europese Commissie de kwetsbare positie van nieuwsuitgevers op de online advertentiemarkt erkent. Dit is onder meer aanleiding geweest voor het *European Democracy Shield*, waarmee wordt ingezet op duurzame bescherming van Europese nieuwsuitgevers.

Herkent u, net als de Europese Commissie, het belang om de positie van nieuwsuitgevers binnen Omnibus Digitaal extra te beschermen ten opzichte van grote (Amerikaanse) techbedrijven? Deze leden ontvangen graag een toelichting.

Antwoord

Het kabinet onderschrijft het belang van onafhankelijke journalistiek en is zich bewust van het belang van advertentie-inkomsten voor de financiering en onafhankelijkheid van de journalistiek. Aanbieders van mediadiensten zijn uitgezonderd van het voorgestelde artikel over gecentraliseerde consentinstellingen. Deze uitzondering is opgenomen vanwege het belang van online-inkomstenstromen voor onafhankelijke journalistiek als onmisbare pijler van een democratische samenleving en zodat mediadiensten rechtstreeks met gebruikers kunnen communiceren om hen te informeren en toestemmingskeuzes te laten maken.³⁰ Het kabinet is deze uitzondering nader aan het bestuderen. De EDPB en EDPS hebben in hun advies van 10 februari jl. aanbevolen om deze uitzondering te heroverwegen, omdat deze uitzondering niet zou bijdragen aan het tegengaan van *consent fatigue*, en omdat aanbieders van mediadiensten bij de verwerking van persoonsgegevens in het kader van cookies vaak samenwerken met derde partijen.

93

De Europese Commissie poogt nieuwsuitgevers binnen de Omnibus Digitaal te beschermen door hen uit te zonderen van gecentraliseerde cookie-toestemming voor de verwerking van persoonsgegevens (art. 88ter, lid 3). Deze uitzondering voor mediadiensten is noodzakelijk om te voorkomen dat het financieren van journalistiek middels advertenties nagenoeg onmogelijk wordt, maar de invoering van 'één klik' (art. 88bis, lid 4, sub a) leidt er alsnog toe dat de financiering van de journalistiek volgens NPD Nieuwsmedia ernstig in gevaar wordt gebracht. De gecentraliseerde cookie-toestemming vergroot de marktmacht van grote (Amerikaanse) techbedrijven. Hoewel zij op grote schaal data verzamelen en persoonsgericht adverteren, zullen zij minder geraakt worden door dit voorstel, omdat ze in mindere mate gebruik van cookie-toestemming bij hun dataverzameling en targeting.

Herkent u het risico dat de voorgestelde maatregelen binnen de Omnibus Digitaal de marktmacht van grote (Amerikaanse) techbedrijven op de online advertentiemarkt juist verder vergroot, terwijl grote (Amerikaanse) techbedrijven door steeds groter wordende marktmacht de duurzame financiering van de Nederlandse journalistiek bedreigt? Deze leden ontvangen graag een toelichting.

Antwoord

In het voorstel is een uitzondering opgenomen voor aanbieders van mediadiensten, waardoor het artikel over gecentraliseerde consentmechanismen op hen geen betrekking heeft. Het kabinet onderzoekt deze uitzondering nog. Hierbij onderzoekt het kabinet ook of er een risico is dat grote platforms in de praktijk mogelijk een bepalende rol krijgen bij de interpretatie of toepassing van de definitie van het begrip *media service providers*, of dat het feit dat dit risico voldoende is ingeperkt doordat het voorstel aansluit bij de bestaande definitie hiervan in Verordening (EU) 2024/1083 (Europese verordening mediavrijheid).

³⁰ Paragraaf 1, COM 2025(837) final.

94

Tot slot hebben de leden van de fractie van GroenLinks-PvdA van NDP Nieuwsmedia vernomen dat zij verwachten dat de uitzondering in de praktijk ertoe zal leiden dat grote Amerikaanse techbedrijven (zoals Google) bepalen wat kan worden gekwalificeerd als *media service provider* in de zin van de Media Freedom Act. Dit vergroot de marktmacht van de digitale gatekeepers, zoals bedoeld in de Digital Markets Act (DMA).

Erkent u dit risico? Zo nee, waarom niet? Zo ja, acht u het wenselijk om hier iets aan te doen? Deze leden ontvangen graag een toelichting.

Antwoord

Hiervoor verwijs ik u naar de beantwoording van vraag 93.

95

Bezwaarmogelijkheden burgers

Met de wijzigingen van de AVG waarin de Omnibus Digitaal voorziet wordt het recht om bezwaar te maken tegen de verwerking van persoonsgegevens van artikel 21 van de AVG beperkt, nu de bewijslast en de drempels verschuiven. Het trainen van AI wordt bijvoorbeeld vaker aangemerkt als een gerechtvaardigd belang. Burgers moeten in dat geval aantonen dat hun concrete privacybelang zwaarder weegt dan het innovatiebelang van het bedrijf. Dat vormt een aanzienlijk hogere drempel dan tot nu toe het geval was.

Hoe oordeelt u over de wijzigingen ten aanzien van de bezwaarmogelijkheden van burgers en maatschappelijke organisaties?

Antwoord

Zoals in antwoord 64 toegelicht, zou het voorgestelde artikel 88c het voor betrokkenen moeilijker kunnen maken om te betwisten dat er een gerechtvaardigd belang is. Zoals aldaar opgemerkt, kunnen betrokkenen weliswaar bezwaar maken tegen de verwerking van persoonsgegevens (opt-out), maar bestaat het risico dat betrokkenen vaak niet weten wanneer of door wie hun gegevens worden gebruikt voor AI-trainingsdoeleinden, of dat zij bij tal van bedrijven bezwaar zouden moeten maken om gegevensverwerking te voorkomen. De EDPB en de EDPS vinden het voorgestelde artikel 88c onnodig en niet verhelderend. Mocht het artikel worden doorgezet, dan bevelen EDPB en EDPS onder meer aan om te verduidelijken dat het recht op bezwaar, indien mogelijk en ruim tevoren, onder de aandacht van de betrokkenen moet worden gebracht, zodat betrokkenen vanaf het begin dit recht kunnen uitoefenen. Wat betreft het kabinet is in het voorgestelde artikel 88c de balans tussen de rechten van betrokkene en de mogelijkheden om persoonsgegevens te verwerken niet goed getroffen.

96

De EDPB en EDPS waarschuwen dat burgers niet meer kunnen overzien waar hun gegevens terechtkomen als het trainen van AI automatisch als 'gerechtvaardigd belang' wordt aangemerkt.

Hoe oordeelt u over deze zorgelijke conclusie van de EDPB en EDPS? Deze leden ontvangen graag een toelichting.

Antwoord

Zoals aangegeven in de beantwoording van vraag 64 deelt het kabinet de zorgen van de EDPB en EDPS dat dit voorstel zo zou kunnen worden opgevat dat de ontwikkeling en exploitatie van AI in principe als een gerechtvaardigd belang moet worden beschouwd.

97

Hoe beoordeelt u de kritiek op dit onderwerp van onafhankelijke organisaties en consumentenbonden, zoals BEUC en Corporate Europe Observatory³¹?

Antwoord

BEUC betreurt de plannen van de Commissie om bedrijven toe te staan persoonsgegevens te gebruiken voor de ontwikkeling en exploitatie van een AI-systeem zonder toestemming van de consument te vragen, onder meer omdat deze wijziging alleen bedrijven met toegang tot grote datasets ten goede zou komen, terwijl de concurrentie met Europese start-ups verder wordt verstoord en de consument wordt benadeeld. Voor het oordeel van het kabinet hierover verwijs ik naar antwoord 64 en 66.

Zoals aangegeven in het antwoord op vraag 18 zijn de voorgestelde wijzigingen die in het artikel van Corporate Europe Observatory³² worden benoemd zijn over het algemeen wijzigingen waar het kabinet kritisch op is of zorgen over heeft omdat ze doelen van de wetgeving afzwakken, afbreuk doen het niveau van gegevensbescherming en in veel gevallen niet lijken bij te dragen aan het verlagen van de regeldruk. Dit is in het BNC-fiche over de voorstellen toegelicht.

98

De leden van de fractie van GroenLinks-PvdA lezen dat de Omnibus Digitaal voorziet in een beperking van de reikwijdte van de bevoegdheid van overheden om gegevens op te vragen bij bedrijven in situaties van 'uitzonderlijke noodzaak' tot alleen 'algemene noodsituaties'. Dit is volgens de regering een verbetering voor het recht op gegevensbescherming.

Kunt u aangeven wat deze aanpassing betekent voor (mede)overheden? In welke situaties van 'uitzonderlijke noodzaak' kunnen (mede)overheden nu geen informatie meer opvragen? Deze leden ontvangen graag een toelichting met een aantal voorbeelden.

Antwoord

³¹ The European Consumer Organisation (BEUC), 'EU's plan to simplify digital laws to benefit mainly large companies at the expense of consumers', 19 november 2025, <https://www.beuc.eu/press-release/eus-plan-simplify-digital-laws-benefit-mainly-large-companies-expense-consumers>; en Corporate Europe Observatory, 'Article by article, how Big Tech shaped the EU's roll-back of digital rights', 14 januari 2026, <https://corporateeurope.org/en/2026/01/article-article-how-big-tech-shaped-eus-roll-back-digital-rights>.

³² Article by article, how Big Tech shaped the EU's roll-back of digital rights | Corporate Europe Observatory

De beperking van de reikwijdte van de bevoegdheid van overheden om gegevens op te vragen bij bedrijven in situaties van 'uitzonderlijke noodzaak' tot alleen 'algemene noodsituaties' betekent voor (mede)overheden dat ze nu geen informatie meer mogen opvragen in situaties waarin geen sprake is van een 'algemene noodsituatie', maar waar sprake is van het opvragen van gegevens waarvan het ontbreken haar ervan weerhoudt een bij wet opgelegde specifieke taak van algemeen belang te vervullen en alle andere middelen waarover zij beschikt om dergelijke gegevens te verkrijgen heeft uitgeput. Voorbeelden zijn niet beschikbaar, omdat een dergelijke situatie van 'uitzonderlijke noodzaak' nog niet is voorgekomen (zie antwoord op vraag 99).

99

Kunt u aangeven hoe vaak dit soort situaties van 'uitzonderlijke noodzaak' in de afgelopen jaren zijn voorgekomen?

Antwoord

Voor zover bekend is een dergelijke situatie tot op heden nog niet voorgekomen.

100

Kunt u een inschatting geven van de effecten van deze aanpassing?

Antwoord

Het effect van deze aanpassing is dat de beperking tot "algemene noodsituaties" het aantal gevallen waarin overheden informatie bij bedrijven kunnen opvragen zal beperken, omdat "algemene noodsituatie" duidelijk is gedefinieerd in de verordening.

101

Past deze aanpassing in de actuele strategie om minder afhankelijk te worden van de grote (Amerikaanse) techbedrijven? Deze leden ontvangen graag een toelichting.

Antwoord

Deze voorgestelde aanpassing is niet direct relevant voor het versterken van de digitale open strategische autonomie.

102

In het BNC-fiche lezen deze leden dat er ook mogelijke effecten zijn voor de rechtspraak. Welke effecten, en in welke omvang, worden door u voorzien? Wat is het oordeel van de partijen in de rechtspraak wat betreft de effecten van deze aanpassingen?

Antwoord

In het algemeen verwacht het kabinet niet dat de omnibussen grote gevolgen hebben voor de rechtspraak, omdat veel voorgestelde wijzigingen in lijn met de kabinetsinzet wetgeving versimpelen, terwijl de doelen van de wetgeving daarbij in stand blijven. Het versimpelen van de regels kan ook interpretatie, naleving en handhaving van wetgeving vergemakkelijken. Specifiek voor een aantal voorgestelde aanpassingen aan de AVG, zoals de gewijzigde definitie van

persoonsgegevens, verwacht het kabinet wel dat deze tot meer belasting bij de rechtspraak kan leiden als deze ongewijzigd blijven. Het kabinet heeft niet op basis van het voorstel advies aan de rechtspraak gevraagd. Dit gebeurt bij het opstellen van uitvoeringswetgeving waarbij gevolgen voor de rechtspraak worden verwacht.

103

De leden van de fractie van GroenLinks-PvdA hebben van IPO en de VNG vernomen dat zij zich zorgen maken over risico's op surveillance bij bias-detectie, de gelijkschakeling van commerciële AI- training met wetenschappelijk onderzoek en de verschuiving van verantwoordelijkheid voor AI-geletterdheid. IPO en VNG wezen ook op mogelijke versnippering van toezicht, het schrappen van de registratieplicht voor AI-systemen, onduidelijkheid over gecentraliseerde incidentrapportage en de inperking van lokaal ethisch beleid.

Kunt u op alle genoemde punten inhoudelijk reageren? Hoe oordeelt u op deze kritiekpunten? Deze leden zien graag een reactie op de inperking van (decentraal) ethisch beleid.

Antwoord

Het kabinet deelt veel van de zorgen van de VNG en de IPO. Zie voor de positie van het kabinet ten aanzien van bias-detectie en AI-training het antwoord op vraag 12, voor gecentraliseerde incidentmeldingen het antwoord op vraag 25 en voor het schrappen van de registratieplicht het antwoord op vragen 38 tot en met 43.

Met betrekking tot AI-geletterdheid steunt het kabinet de doelstelling om AI-geletterdheid te bevorderen bij personeel dat met AI werkt. Tegelijkertijd erkent het kabinet dat de huidige verplichting in de AI-verordening onvoldoende duidelijk is en onzekerheid kan creëren bij deze organisaties. Het kabinet steunt daarom inspanningen om deze verplichting te verduidelijken of organisaties bij het voldoen aan deze verplichting te ondersteunen.

104

In het BNC-fiche lezen de leden van de fractie van GroenLinks-PvdA dat de regering kritisch is op het voorstel om de P2B-verordening gefaseerd in te trekken. Wat is de strategie om dit onderdeel van de Digitale Omnibussen aangepast te krijgen?

Antwoord

Het kabinet steunt het doel om platformwetgeving te versimpelen, maar is van mening dat het vrijwel volledig schrappen van de regels in de P2B te rigoureus is en pleit daarom in het kader van vereenvoudiging voor een meer gerichte en evenredige aanpak. Een deel van de bepalingen uit de P2B is complementair aan de Digitale marktenverordening (DMA) en de Digitale dienstenverordening (DSA). Het schrappen van deze bepalingen leidt tot verlies aan rechtszekerheid voor ondernemers die hun goederen of diensten aanbieden via kleinere platforms. Dat terwijl de vermindering van administratieve lasten met het schrappen van de P2B-verordening marginaal is. Volgens het kabinet staat het verlies aan bescherming

niet in verhouding tot de vermindering van administratieve lasten die daarmee zou worden bereikt. Door een gerichtere aanpassing kan het regelgevingskader worden gestroomlijnd met behoud van de bescherming die de P2B-verordening biedt aan zakelijke gebruikers van platforms.

De inzet van het kabinet is daarom om de bepalingen uit de P2B die complementair zijn aan de DMA en de DSA en het toezicht hierop te behouden. Het kabinet richt zich daarbij primair op de belangrijkste transparantieverplichtingen voor platforms op het gebied van bijvoorbeeld rangschikking (artikel 5) en gedifferentieerde behandeling (artikel 7). Het kabinet trekt hierbij gezamenlijk op met lidstaten die eveneens kritisch staan tegenover het volledig schrappen van de P2B-verordening. Samen met een aantal lidstaten is een non-paper verspreid waarin de hierboven genoemde zorgen zijn toegelicht.

105

Hoe ligt het Europese krachtenveld ten aanzien van deze aanpassingen?

Antwoord

De meeste lidstaten lijken het voorstel van de Commissie om de P2B-verordening te schrappen, te steunen. Tegelijkertijd stelt een aantal lidstaten zich kritisch op. Zoals in het antwoord op vraag 105 uiteengezet, heeft Nederland met een aantal van deze lidstaten een non-paper geschreven waarin wordt voorgesteld een aantal bepalingen (voorwaardelijk) te behouden. De inzet van deze non-paper is om de discussie op Europees niveau te voeden. Mogelijk leidt dit nog tot aanpassingen van het huidige compromisvoorstel in de Raad.

106

Is aanpassing van dit onderdeel een harde randvoorwaarde om in te kunnen stemmen met de Omnibus Digitaal?

Antwoord

Het kabinet beoordeelt de uitkomsten van de onderhandelingen op de digitale omnibus in verhouding tot de Nederlandse inzet in zijn geheel. Daarbij is de inzet van het kabinet op dit onderdeel om voldoende waarborgen te treffen om de gewenste vereenvoudiging op gebied van platformregulering door te kunnen zetten. Zolang aan die zorgen tegemoet wordt gekomen, is het in de bredere context van de omnibus geen harde randvoorwaarde om op dit onderdeel tot tekstaanpassingen te komen.

107

De ACM is sinds kort bevoegd om de P2B te handhaven en ontvangt, zo lezen deze leden in het BNC-fiche, inmiddels regelmatig meldingen over niet-naleving van de P2B door platforms: *"Zonder de P2B kan de ACM geen toezicht meer houden op problemen die ondernemers ondervinden op platforms die buiten Nederland gevestigd zijn"*. Schrappen zal dus naar verwachting leiden tot minder rechtszekerheid en minder bescherming voor met name kleinere ondernemers die handelen op platforms.

Kunt u, in overleg met ACM, een nadere toelichting geven op welk type bedrijven zich niet aan de wetgeving houdt?

Antwoord

De P2B is van toepassing op alle onlinetussenhandelsdiensten en zoekmachines wanneer zij ondernemingen de mogelijkheid bieden om goederen of diensten aan consumenten via hen aan te bieden. Dat betekent dat de P2B voor verschillende soorten platforms in diverse sectoren en/of markten geldt, bijvoorbeeld online marktplaatsen, reserveringsplatforms, sociale media platforms of vergelijkingssites. De reikwijdte van de P2B is daarom erg groot. Mede daarom heeft de ACM in 2023 een leidraad gepubliceerd om de bekendheid van de P2B te vergroten.

Net als bij alle andere wetten waar de ACM toezicht op houdt, werkt de ACM met betrekking tot de naleving van de P2B ook meldingsgestuurd. De ACM ontvangt regelmatig meldingen en handavingsverzoeken van ondernemingen die een beroep doen op de P2B. De ACM kan geen uitspraken doen over het type online platforms waar de ACM al dan niet overtredingen van de P2B heeft geconstateerd.

108

Kunt u, in overleg met ACM, toelichting geven op de verwachte impact van het schrappen van de P2B?

Antwoord

De P2B beschermt ondernemers wanneer zij zaken doen met platforms, ongeacht hun omvang, en draagt bij aan een eerlijke en voorspelbare bedrijfsomgeving. De P2B biedt daarvoor een reeks waarborgen, die vooral van belang zijn voor ondernemers die op online platforms goederen en diensten aanbieden. Deze waarborgen zien met name op de transparantie die online platforms moeten geven over bijvoorbeeld het opschorten, beperken van accounts en het interne klachtenafhandelingssysteem. Juist de mate van concreetheid van de P2B is voor deze ondernemers van belang.

Het schrappen van de P2B betekent dat bepaalde beschermingsmaatregelen voor zakelijke gebruikers van digitale platforms komen te vervallen. Weliswaar biedt de DSA in sommige gevallen ook bescherming tegen bepaalde gedragingen van online platforms, maar het niveau van bescherming die de P2B biedt gaat verder. Zonder de waarborgen van de P2B kunnen online platforms bijvoorbeeld hun voorwaarden zonder of met slechts een minimale waarschuwing wijzigen, wat onevenredige gevolgen kan hebben voor bedrijven (vooral het mkb) die afhankelijk zijn van de toegang tot die platforms. Als gevolg lopen ondernemers het risico minder goed beschermd te zijn in hun commerciële relatie met dergelijke online platforms.

Dankzij de P2B kan de ACM ook problemen oplossen die spelen op online platforms die buiten Nederland gevestigd zijn. Door het schrappen van de P2B kunnen ondernemers in veel gevallen niet meer terecht bij de ACM voor handhaving naar aanleiding van klachten over platforms, ongeacht waar deze gevestigd zijn. Dit doet volgens het kabinet af aan de rechtszekerheid van de

gebruikers van die platforms. Het kabinet wil deze risico's mitigeren door in te zetten op behoud van de P2B-bepalingen die voor ondernemers het meest van belang zijn en de publieke handhaving daarvan door de nationale autoriteiten van lidstaten.

Het schrappen van de P2B is niet direct van invloed op de mate van digitale autonomie van Nederlandse ondernemers of de afhankelijkheid van techbedrijven. Ten aanzien van de grootste online platforms geldt namelijk dat de verplichtingen in de DMA en DSA onverkort van kracht blijven. De DMA en DSA bieden in veel gevallen verdergaande bescherming tegen oneerlijke praktijken van de grootste online platforms. Desondanks kan het schrappen van de P2B er wel toe leiden dat Nederlandse ondernemers tot op zekere hoogte handelingsperspectief verliezen in hun afhankelijkheidsrelatie tot online platforms.

109

Past deze aanpassing in de actuele strategie om minder afhankelijk te worden van de grote (Amerikaanse) techbedrijven? Deze leden ontvangen graag een toelichting.

Antwoord

Zoals in het antwoord op de voorgaande vraag toegelicht, houdt het voorstel tot het schrappen van de P2B geen verband met de doelstellingen rond digitale autonomie en het verminderen van de afhankelijkheid van de grootste techbedrijven. Met het schrappen van de P2B verliezen zakelijke gebruikers van platforms tot op zekere hoogte handelingsperspectief in hun afhankelijkheidsrelatie met online platforms, waaronder die van de grotere techbedrijven. Tegelijkertijd bieden de regels in de DMA en DSA ondernemers onverkort bescherming in hun relatie tot de grootste online platforms.

110

De leden van de fractie van GroenLinks-PvdA hebben grote zorgen over de uitzonderingen die in de Omnibus Digitaal worden geïntroduceerd met betrekking tot de bepalingen inzake het overstappen tussen clouddiensten. Overstappen is niet in alle gevallen meer gratis, maar er kunnen 'proportionele overstapvergoedingen' in rekening worden gebracht bij maatwerk-diensten. In het BNC-fiche lezen de leden dat deze uitzonderingen volgens de regering juist onduidelijkheid voor gebruikers van clouddiensten creëren en hun keuzevrijheid belemmeren. De regering ziet *"liever geen aanpassingen die de werking van dit onderdeel van de Dataverordening beperken of vertragen gezien de Dataverordening een belangrijk onderdeel is in het beter laten functioneren van de Europese cloudmarkt"*.

Wat is de strategie om dit onderdeel van de Omnibus Digitaal aangepast te krijgen?

Antwoord

Het kabinet brengt haar standpunt op dit onderdeel in bij de onderhandelingen dit op dit moment lopen. Het kabinet zet daarbij in op het verwijderen van de

geïntroduceerde uitzondering voor op gemaakte clouddiensten. Daarbij zoekt het kabinet steun bij gelijkgestemde lidstaten.

Ons kenmerk
DGED / 104349249

111

Hoe ligt het Europese krachtenveld ten aanzien van deze aanpassingen?

Antwoord

Op het moment dat deze vragen werden beantwoord zijn deze specifieke aanpassingen nog weinig besproken in de onderhandelingen. Het is daarom nog niet mogelijk het krachtenveld te schetsen, maar verschillende lidstaten lijken open te staan voor de Nederlandse inzet op dit punt.

112

Is aanpassing van dit onderdeel een harde randvoorwaarde om in te kunnen stemmen met de Omnibus Digitaal?

Antwoord

Het kabinet zal de uiteindelijke Omnibus Digitaal in zijn geheel wegen en op basis daarvan bepalen of zij met de Omnibus Digitaal kan instemmen.

113

Past deze aanpassing in de actuele strategie van Europa om minder afhankelijk te worden van de grote (Amerikaanse) techbedrijven? Deze leden ontvangen graag een toelichting.

Antwoord

Het kabinet ziet de voorgestelde aanpassingen in de bepalingen die overstappen tussen clouddiensten mogelijk maken als onwenselijk. Deze mening deelt zij met de ACM, in Nederland de toezichthouder op de bepalingen uit de Dataverordening die zien op cloud. Door de geïntroduceerde uitzondering voor maatwerkdiensten ontstaat het risico dat de doelstellingen van de Dataverordening op het gebied van cloud, namelijk verbeterde interoperabiliteit en portabiliteit, worden ondermijnd.

Vanwege de aard van de cloudmarkt zou een groot deel van de aangeboden diensten onder de uitzondering kunnen vallen, wat zou leiden tot hogere drempels voor overstappen in vergelijking met de oorspronkelijke tekst van de Dataverordening. Deze uitzondering brengt juridische onzekerheid voor gebruikers van clouddiensten met zich mee. Dit zou de inspanningen om de portabiliteit en interoperabiliteit van clouddiensten te bevorderen belemmeren. Daarom stellen wij voor om het voorgestelde artikel 31 (1a) te schrappen.

Door overstapbelemmeringen weg te nemen en interoperabiliteit te bevorderen verkleinen we onze afhankelijkheden van individuele cloudbedrijven. Dit biedt zowel voor de bredere Europese interne markt als voor individuele eindgebruikers mogelijkheden om afhankelijkheden af te bouwen.

114

De leden van de fractie van GroenLinks-PvdA merken op dat de verantwoordelijkheden omtrent AI-geletterdheid worden gewijzigd. De verplichtingen voor bedrijven om AI-geletterdheid te bevorderen worden verminderd. Deze verplichting geldt voortaan alleen voor organisaties die hoog risico AI-systemen inzetten. MBK-bedrijven worden grotendeels vrijgesteld van een actieve plicht om personeel te trainen. De verantwoordelijkheid om de algemene bevolking AI-geletterd te maken, wordt sterker bij de lidstaten zelf gelegd. Er wordt meer ruimte gegeven aan vrijwillige gedragscodes. In plaats van strikte wettelijke eisen voor training, mogen sectoren zelf bepalen wat een "voldoende niveau" van geletterdheid is voor hun specifieke werknemers. In het BNC-fiche lezen deze leden dat de regering bezwaren heeft tegen het schrappen van de registratieplicht voor hoog risico AI die alleen voor beperkte of procedurele taken worden gebruikt omdat dit de transparantie verlaagt over het gebruik van AI-systemen in hoog risico context en het toezicht bemoeilijkt op deze systemen. Bovendien levert deze maatregel slechts een beperkte verlichting van regeldruk op, aldus de regering. De leden van de fractie van GroenLinks-PvdA maken zich zorgen over de effecten hiervan.

Wat is volgens u het effect hiervan? Deze leden ontvangen graag een toelichting.

Antwoord

Voor de beoordeling van het kabinet van het commissievoorstel voor de aanpassing van de AI-geletterdheid verplichting, verwijs ik u naar het antwoord op vraag 103. Voor het effect van het voorstel om de registratieplicht te schrappen voor hoog-risico AI die alleen voor beperkte of procedurele taken worden gebruikt, verwijs ik u naar het antwoord op vragen 38 t/m 43.

115

Wat is het standpunt van u ten aanzien van deze wijzigingen? Deze leden ontvangen graag een toelichting.

Antwoord

Voor de beoordeling van het kabinet van het commissievoorstel voor de aanpassing van de AI-geletterdheid verplichting, verwijs ik u naar het antwoord op vraag 103. Voor de beoordeling van het voorstel om de registratieplicht te schrappen voor hoog-risico AI die alleen voor beperkte of procedurele taken worden gebruikt, verwijs ik u naar het antwoord op vragen 38 t/m 43.

116

Hoe denkt u deze verantwoordelijkheid binnen Nederland, samen met de medeoverheden, in te gaan vullen?

Antwoord

In het kader van de AI-verordening voeren de koepels van de medeoverheden, in samenwerking met BZK, een Uitvoerbaarheidstoets Decentrale Overheden (UDO)

traject uit.³³ Dit om de (financiële) consequenties van deze wetgeving in kaart te brengen. Hierin is ook aandacht voor AI-geletterdheid. Daarnaast worden er in het kader van AI-geletterdheid meerdere acties ondernomen, zoals de verkenning van een overheidsbreed AI-competentiecentrum als een van de versnellers van de NDS-prioriteit AI. Bij het overheidsbreed versterken van AI-geletterdheid werken overheden daarbij al samen en worden vanuit BZK ondersteunende hulpmiddelen ontwikkeld en samengebracht. Ook biedt de Rijksacademie voor Digitalisering en Informatisering Overheid (RADIO) sinds dit jaar de basiscursus AI aan voor ambtenaren.

117

De EDPB en de EDPS hebben in een gezamenlijke opinie over de Omnibus AI bepleit dat bedrijven zelf verantwoordelijk dienen te blijven voor het waarborgen van voldoende kennis en zorgvuldigheid binnen hun organisatie.

Hoe oordeelt u over het advies van de EDPB en de EDPS? Deze leden ontvangen graag een toelichting.

Antwoord

Voor de beoordeling van het kabinet van het commissievoorstel voor de aanpassing van de AI-geletterdheid verplichting, verwijs ik u naar het antwoord op vraag 103.

118

In het BNC-fiche lezen de leden van de fractie van GroenLinks-PvdA dat het de regering specifiek over het voorstel in de Omnibus Digitaal om een Europees meldpunt in te richten zorgen heeft over de subsidiariteit. De motivatie hiervoor is als volgt verwoord: *"Het specifieke doel van versimpelen en stroomlijnen van de verschillende meldplichten uit (cyber)wetgeving kan voor een groot deel ook zonder dit vergaande middel bereikt worden en ook op nationaal niveau door lidstaten 12 worden opgelost. Zo zal de grootste groep entiteiten onder de CER- en de NIS2-richtlijn niet grensoverschrijdend opereren. Deze partijen hebben voldoende aan het simplificeren van rapportageverplichtingen en een meldpunt op nationaal niveau. Bovendien wordt er door lidstaten in diverse Europese expertgroepen, waaronder de NIS Cooperation Group, reeds samengewerkt om dit doel te bereiken".*

Kunt u een nadere toelichting geven over de zorgen ten aanzien van de subsidiariteit? Is er volgens u wel of niet sprake van strijdigheid met het subsidiariteitsbeginsel op dit onderdeel?

Antwoord

Het kabinet acht het van belang om te benadrukken dat de EU mag optreden voor zover het overwegen optreden niet of onvoldoende door de lidstaten zelf kan worden verwezenlijkt. Lidstaten, waaronder Nederland, hebben al goed

³³ Zie bijvoorbeeld de impactanalyse die de VNG uitvoerde in opdracht van BZK: [250116 VNG-Uitvoeringsanalyse-Digital-Decade-AI-verordening vdef](#).

functionerende meldpunten, waarbij bijvoorbeeld ook wordt voorzien in waarborgen voor het veilig ontvangen van incidentmeldingen. Dat betekent concreet dat de gevraagde doelstelling voldoende door afzonderlijk optreden van de lidstaten zelf geregeld kan worden en optreden op EU-niveau niet nodig én niet gerechtvaardigd is. Hierdoor is er sprake van strijdigheid met het subsidiariteitsbeginsel en dat is ook waar de zorgen van het kabinet in zitten: de Commissie heeft niet inzichtelijk gemaakt waarom de nationale meldstructuren ontoereikend zouden zijn en het op Europese schaal verzamelen van informatie noodzakelijk is. Ook zal blijken, afhankelijk van hoe het Europees meldpunt zal worden ingericht, of dit voorstel effectief zal bijdragen aan het verlagen van regeldruk en of nationale competenties rondom nationale veiligheid mogelijk worden aangetast.

120

De leden van de fractie van GroenLinks-PvdA merken op dat de Digital Fairness Act (DFA) enerzijds, en de Omnibus Digitaal en de Omnibus AI anderzijds, deel uitmaken van een bredere beweging van de Europese Commissie om de digitale regelgeving te moderniseren, maar ze hebben tegenovergestelde doelen. Waar de DFA nieuwe regels toevoegt om consumenten te beschermen, zijn de Omnibus Digitaal en de Omnibus AI juist gericht op het verminderen van regeldruk (deregulering). De DFA voegt een nieuwe laag bescherming toe. Volgens de Europese Commissie is dit nodig omdat de huidige wetten (zoals de Unfair Commercial Practices Directive) "gaten" vertonen bij het aanpakken van moderne digitale problemen zoals *dark patterns* en verslavende algoritmes.

Hoe beoordeelt u deze tegenstelling? Deze leden ontvangen graag een toelichting.

Antwoord

Het doel van de omnibussen is om bestaande wetgeving te versimpelen. Deze omnibussen richten zich daarbij specifiek op een subset van digitale wetgeving. Sommige van deze wetgeving draagt bij aan online consumentenbescherming, maar dit is niet het primaire doel van deze wetgeving. Het feit dat er bij deze bestaande digitale wetgeving wordt gekeken of de regeldruk kan worden verlaagd staat niet haaks op het feit dat er wordt gekeken of er – eventueel via nieuwe wetgeving – maatregelen kunnen worden genomen om specifieke problemen omtrent online consumentenbescherming te adresseren.

121

Wordt met de Omnibus Digitaal en de Omnibus AI de doelstelling van de Digitale Fairness Act (DFA) aangetast? Zo ja, bij welke aanpassingen is dit volgens u aan de orde?

Antwoord

Zoals in de beantwoording van vraag 120 aangegeven doen de omnibussen in het algemeen niets af aan de doelstellingen van de aangekondigde DFA. Het vorige kabinet heeft de Commissie in een non-paper opgeroepen om de DFA als gerichte maatregel in te zetten voor de aanpak van een aantal specifieke schadelijke online handelspraktijken. Een belangrijk onderdeel van de inzet is het creëren van meer samenhang tussen het consumentenrecht enerzijds en regelgeving zoals de DSA

anderzijds. Hierdoor ontstaan een Europees geharmoniseerd kader en kan inconsistentie en verdere fragmentatie worden tegengegaan.

Wel bevat, zoals in het BNC-fiche^[1] aangegeven, het voorstel voor de Omnibus Digitaal een aantal wijzigingen aan de AVG die afbreuk doen aan het recht op privacy en gegevensbescherming. Deze voorgestelde wijzigingen kunnen daarmee wel een negatief effect hebben op de bescherming van consumenten online. Het kabinet zet erop in dat de omnibussen geen afbreuk doen aan de bescherming van grondrechten.

Vragen en opmerkingen van de leden van de fractie van de BBB

1

Wat is de totale geraamde besparing in administratieve lasten – uitgedrukt in euro's en fulltime-equivalenten (fte) – als gevolg van de Omnibus Digitaal en de Omnibus AI voor Nederlandse bedrijven in de komende vijf jaar?

Antwoord

Zoals aangegeven in het SWD voor de omnibusvoorstellen verwacht de Europese Commissie dat de voorstellen zullen leiden tot een lastenreductie van €1,3 miljard per jaar voor bedrijven en een lastenreductie van €330 miljoen per jaar voor overheden.³⁴

2

Is er of wordt er een onafhankelijke impact assessment uitgevoerd op de Nederlandse situatie? Zo ja, kunt u deze impact assessment aan de Kamer doen toekomen?

Antwoord

Een onafhankelijk impact assessment voor de Nederlandse situatie wordt niet voorzien. Dit wordt ook bemoeilijkt omdat het voorstel gezien het tempo van de onderhandelingen voortdurend aan verandering onderhevig is. Het kabinet heeft de Europese Commissie verzocht uitgebreidere analyse van de impact van de voorstellen te presenteren, hecht belang aan de adviezen van de EDPS in samenspraak met de EDPB en brengt zelf de gevolgen van de voorstellen verder in kaart.

3

Hoe waarborgt u dat de versoepelingen niet leiden tot een lagere bescherming van fundamentele rechten met betrekking tot privacy?

Antwoord

Voorstellen met risico's voor grondrechten dienen, op basis van grondige analyse, te worden behandeld op een wijze die recht doet aan de zorgpunten en in het bijzonder de potentiële impact op grondrechten. De impact op grondrechten weegt

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

³⁴ SWD(2025) 836 final, Annex II

voor het kabinet zwaar in haar oordeel over dit voorstel. Het kabinet is daarom kritisch op voorstellen die zouden leiden tot een lager beschermingsniveau.

4

Op welke wijze wordt na invoering van de zevende omnibus ervoor gezorgd dat belanghebbenden op de hoogte zijn en worden getraind?

Antwoord

De verschillende wetten die de omnibussen wijzigt zijn voor verschillende groepen belanghebbenden relevant. Rondom de verschillende wetten wordt al gecommuniceerd richting belanghebbenden. Voor wetten die al zijn uitgevoerd is het de taak van de toezichthouder om belanghebbenden van voorlichting en informatie te voorzien. Communicatie over de uiteindelijke wijzigingen over de omnibussen zal daarom waarschijnlijk ook gebeuren via de communicatie over de onderliggende wetten. De toezichthouders op deze wetten hebben hier ook een belangrijke rol in. Het kabinet verwacht niet dat er als gevolg van wijzigingen in de omnibussen die wetgeving versimpelen specifieke nieuwe trainingen nodig zijn.

5

Is bij de berekening van besparingen rekening gehouden met deze kosten in tijd en geld?

Antwoord

Dat is niet geheel duidelijk uit het SWD. Er staat in het SWD geen expliciete indicatie van extra kosten als gevolg van de wijzigingen. Het primaire effect van de voorstellen zal een lastenreductie zijn. Zoals aangegeven in het antwoord op vraag 4 van uw fractie verwacht het kabinet niet dat er als gevolg van wijzigingen in de omnibussen die wetgeving versimpelen specifieke nieuwe trainingen nodig zijn. Het kabinet verwacht dus ook niet dat daar kosten voor hoeven te worden gemaakt.

6

Welke knelpunten verwacht u bij het MKB en decentrale overheden (gemeenten en provincies) door de wijzigingen van de AI-verordening?

Antwoord

Zoals ook blijkt uit de verwachte lastenverlichting die in het SWD wordt benoemd verwacht ik dat Omnibus AI vooral tot minder regeldruk voor overheden gaat leiden. De Omnibus AI beoogt de naleving van de AI-verordening te versimpelen er zorgt er bovendien voor dat er meer richtsnoeren worden ontwikkeld, die het makkelijker maken aan de regels te voldoen. Ook krijgen onder het voorstel voor de Omnibus AI organisaties meer tijd om zich voor te bereiden op de inwerkingtreding van de hoog-risico bepalingen uit de AI-verordening.

7

Hoe wordt ervoor gezorgd dat AI-leveranciers in Nederland de versoepelde eisen daadwerkelijk toepassen?

Antwoord

Er worden in Nederland toezichthouders aangewezen die toezicht zullen houden op de naleving van de eisen uit de AI-verordening. Indien zij niet-naleving constateren bij een AI-leverancier, kunnen zij via verschillende bevoegdheden, waaronder het opleggen van een sanctie of het van de markt halen van het AI-systeem, naleving alsnog afdwingen.

8

Acht u de voorgestelde inwerkingtredingstermijnen in de beide ontwerp-verordeningen – eenmaal vastgesteld en gepubliceerd – uitvoerbaar voor overheid en bedrijfsleven?

Antwoord

Ik verwacht niet dat dit problemen oplevert. Omnibussen bevatten technische wijzigingen aan bestaande regelgeving, gericht op het verlagen van regeldruk. De implementatie van omnibussen levert dus in principe weinig lasten op. Voor de onderdelen waar dit wel het geval is, zoals bij het Europees meldpunt en de wijzigingen met betrekking tot cookies, gelden ook andere termijnen voor inwerkingtreding, van 6 maanden tot 4 jaar na inwerkingtreding van de Omnibus Digitaal.

9

Worden er pilots voorzien om uitvoerbaarheid te testen?

Antwoord

Het kabinet ziet geen noodzaak pilots te draaien voor de uitvoerbaarheid. Omnibussen bevatten technische wijzigingen aan bestaande regelgeving gericht op het verlagen van regeldruk. Gezien de primaire verwachte impact regeldrukverlaging is, ziet het kabinet geen noodzaak voor afronding van de onderhandelingen hier pilots voor te draaien. De bepalingen van de Omnibus AI zullen tezamen met de gehele AI-verordening in augustus 2029 worden getoetst en geëvalueerd.

10

In welke mate wordt het maatschappelijke middenveld zoals VNG, IPO, en MKB-Nederland betrokken?

Antwoord

Zoals gebruikelijk heeft het kabinet bij en sinds de totstandkoming van het kabinetsstandpunt contact met een brede groep stakeholders, ook uit het maatschappelijk middenveld. De VNG en het IPO zijn daarnaast ook betrokken bij het opstellen van de BNC-fiches.

11

Hoe voorkomt u dat versoepelingen leiden tot een 'race to the bottom' bij AI-veiligheid?

Antwoord

Zoals ook is aangegeven in het BNC-fiche, zet het kabinet er bij de omnibussen op in dat de wetgeving versimpeld, verduidelijkt en gestroomlijnd wordt op een manier waarbij de doelen van de wetgeving overeind blijven. Het kabinet ziet in de huidige omnibusvoorstellen geen voorstellen die AI-veiligheid verlagen, en zet zich ervoor in dat de AI-verordening hetzelfde niveau van bescherming voor de veiligheid, gezondheid en grondrechten behoudt.

12

Wat zijn de risico's op juridische procedures door onduidelijke overgangsregels?

Antwoord

Het kabinet ziet geen concrete risico's op juridische procedures door onduidelijke overgangsregels omdat de primaire verwachte impact van de omnibussen regeldrukverlaging is.

13

Wordt de uitvoerbaarheid getoetst aan de hand van de Nederlandse Digitaliseringsstrategie (NDS)?

Antwoord

De appreciatie van het kabinet van de Omnibussen in het betreffende BNC fiche zijn gebaseerd op het staande kabinetsbeleid, inclusief de NDS. Op beleidsinhoudelijk niveau zijn de doelstellingen en voorgestelde maatregelen van de Omnibussen getoetst aan de NDS.

14

Hoe voorkomt u dat versoepelingen leiden tot meer meldingen bij de AP?

Antwoord

Het kabinet betreft bij de beoordeling van de voorgestelde wijzigingen van de AVG ook de vraag of voorzienbaar is dat deze vermoedelijk zouden leiden tot meer meldingen bij de AP. Dit is één van de redenen waarom het kabinet kritisch is op onder meer de voorgestelde beperking van de definitie van persoonsgegevens en de beperking van het inzagerecht. Er lijkt binnen de Raad steun om deze aanpassingen te schrappen.

15

Voorziet u dat de Europese Commissie advies zal vragen aan de diverse adviesorganen?

Antwoord

Vanwege de rechtsgrondslag voor de omnibussen - voor de Omnibus AI artikel 114 van het Verdrag voor de Werking van de Europese Unie (VWEU) en voor de Omnibus Digitaal artikel 16 en artikel 114 VWEU - zullen in principe beide adviesorganen van de Unie, namelijk het Europees Economisch en Sociaal Comité, en het Comité van de Regio's advies geven. Daarnaast heeft de EDPS al gezamenlijk met de EDPB advies gegeven.

16

Hoe blijft de AVG-compliance gewaarborgd na de voorgestelde wijzigingen?

Ons kenmerk
DGED / 104349249

Antwoord

Het kabinet beoordeelt of de voorgestelde wijzigingen van de AVG bijdragen aan het doel dat de Europese Commissie heeft gesteld, namelijk om de AVG te vereenvoudigen, verduidelijken en harmoniseren zonder kernprincipes of -vereisten uit de AVG aan te tasten of het hoge beschermingsniveau te ondermijnen (Staff Working Document, p. 36-37). Hiermee wordt ook beoogd om de AVG-compliance te waarborgen, want wijzigingen die geen vereenvoudiging of verduidelijking zouden bieden, dragen niet bij aan het bevorderen van de naleving van de AVG.

17

Is er een aparte AVG-impact assessment uitgevoerd voor de Nederlandse situatie?

Antwoord

Er is geen aparte AVG-impact assessment uitgevoerd voor de Nederlandse situatie. Zoals aangegeven in het BNC-fiche weegt de impact van de voorstellen op grondrechten zwaar voor het kabinet. Het kabinet hecht daarom zeer aan het gezamenlijk advies van de EDPB en de EDPS en analyseert zelf de impact van de voorstellen. Gezien de AVG een Europese verordening is, is er geen aanleiding te denken dat de wijzigingen in Nederland een significant andere impact zullen hebben dan in andere lidstaten.

Vragen en opmerkingen van de leden van de fractie van D66, mede namens de leden van de fractie van de PvdD

1

In het BNC-fiche geeft de regering met betrekking tot pijler I aan de nieuwe focus op *data spaces* te waarderen, maar merkt daarbij op dat belangrijke details in de uitwerking nog ontbreken. Ook geeft de regering aan in het voorstel een lange termijn visie te missen over *data spaces*. Wat is in uw ogen de lange termijn visie voor *data spaces*?

Antwoord

Het kabinet heeft de afgelopen jaren het ontwikkelen van *data spaces* financieel ondersteund via nationale subsidies (o.a. het Nationaal Groeifonds) en via co-funding op Europese subsidies (Digital Europe Programma). In de langetermijnvisie van het kabinet wordt ingezet op de zelfredzaamheid van dit soort initiatieven, door middel van het ontwikkelen van een verdienmodel. *Data spaces* hoeven niet winstgevend te zijn, maar wel kostendekkend.

2

Verder wijst de regering erop, met betrekking tot pijler I, dat er nog uitdagingen liggen ten aanzien van het verantwoord delen van data. Deze leden vinden het belangrijk dat data verantwoord wordt gedeeld. Daarom vragen deze leden welke uitdagingen u ziet en hoe deze zich verhouden tot het waarborgen van fundamentele rechten.

Antwoord

De uitdagingen ten aanzien van het verantwoord delen van data in relatie tot pijler I liggen voor het kabinet voornamelijk in het vergroten van het vertrouwen in datadelen tussen bedrijven, waar het niet-persoonlijke data betreft. Juist door het gebrek aan vertrouwen wordt veel data in Europa onvoldoende benut, o.a. voor het trainen van AI.

3

Daarnaast heeft de regering, ten aanzien van dezelfde pijler, nog vragen of er overlap bestaat tussen bestaande activiteiten en de Data Labs. Deze leden vragen of u een beeld heeft van waar die mogelijke overlap plaatsvindt.

Antwoord

De Data Labs zullen de brug vormen tussen data spaces en de AI fabriek. In Nederland lopen verschillende (regionale) initiatieven waar kennis met betrekking tot data voor AI beschikbaar is, denk aan ICAI labs, ELSA labs of AI hubs bij universiteiten. Het is belangrijk om bij het opzetten van het Data Lab in Nederland, als onderdeel van het kenniscentrum van de AI fabriek in Groningen, voort te bouwen op, en te verbinden met, de kennis die in deze hubs beschikbaar is.

4

Gelet op de derde pijler merkt de regering op dat het de inzet op het versterken van partnerschappen met gelijkgestemde landen steunt, onder andere op het gebied van het inzetten van data spaces in internationale datastromen. Deze leden vragen wat u verstaat onder 'gelijkgestemde landen' en hoe u kijkt tegen het verder uitwerken (in EU-verband) van deze term, gelet op het belang dat onze data niet in verkeerde handen komt.

Antwoord

In relatie tot de Data Unie Strategie kan onder 'gelijkgestemde landen' derde landen waarmee op Europees niveau een digitaal partnerschap is afgesloten worden verstaan. Dit zijn op dit moment Japan, Zuid-Korea, Singapore en Canada.

5

De leden van de fractie van D66 onderschrijven dat de regering erop toeziet dat de Europese regelgeving doelgericht en uniform wordt geïmplementeerd, toegepast en gehandhaafd. De leden lezen in het BNC-fiche dat de regering het belang van voldoende capaciteit bij toezichthouders onderstreept. Deze leden vragen of u hiermee doelt op nationale of Europese toezichthouders en of naar uw oordeel de capaciteit momenteel toereikend is. Daarnaast merken de aan het woord zijnde leden op dat de Omnibus Digitaal voorziet in oprichting van een Europees meldpunt dat de rol van nationale toezichthouders lijkt over te nemen. Is er dan nog wel capaciteit bij onze nationale toezichthouder nodig?

Antwoord

Zowel voor nationale als Europese toezichthouders is voldoende capaciteit van belang om effectief toezicht te kunnen houden. Voor de wetten die door deze

omnibussen worden gewijzigd is naar mijn oordeel in het algemeen voldoende capaciteit beschikbaar. Voor de meeste van deze wetten is recent op basis van de uitvoerings- en handhavingstoetsen capaciteit toegekend aan de toezichthouders.

Het kabinet benadrukt dat de rol van de nationale toezichthouders – ongeacht of er een Europees meldpunt wordt ingericht – onverminderd belangrijk is en de capaciteit nog steeds nodig is. De NIS2-richtlijn schrijft namelijk voor dat essentiële entiteiten en belangrijke entiteiten elk significant incident moeten melden bij zowel hun CSIRT (Computer Incident Response Team) als bij de bevoegde autoriteit. Het inrichten van een Europees meldpunt maakt deze verplichting niet anders, immers het CSIRT en de bevoegde autoriteit, met het oog op diens toezichthoudende taken, vervullen beide een andere rol in het stelsel. Hierbij benoemt het kabinet dat met het oog op beide meldingen een meldpunt wordt ingericht én dat voor het doen van de melding bij het CSIRT én bij de bevoegde autoriteit maar één handeling nodig zal zijn.

6

Voorts geeft de regering in het BNC-fiche aan dat het belangrijk is dat er ruimte blijft voor nationale 'flexibiliteit' met betrekking tot het hergebruiken van persoonlijke data in publieke registers. Kunt u verduidelijken wat het in dit kader bedoelt met flexibiliteit?

Antwoord

Met flexibiliteit bedoel ik in dit kader dat de mogelijkheid om bij Algemene Maatregel van Bestuur persoonsgegevens in openbare registers aan te wijzen voor hergebruik. In de Wet hergebruik van overheidsinformatie is nu het uitgangspunt dat dergelijke gegevens niet herbruikbaar zijn, tenzij bij Algemene Maatregel van Bestuur anders is geregeld.

7

Verder lezen de aan het woord zijnde leden in het BNC-fiche dat de Europese Commissie inschat dat de Omnibus AI €297 tot €433 miljoen aan lastenverlichting voor bedrijven oplevert en de Omnibus Digitaal zowel jaarlijks, als eenmalig, €1 miljard. Hoe beoordeelt u de verhouding tussen de mate van lastenverlichting die de Omnibussen opleveren en de beoogde doelen van vereenvoudiging en stroomlijning? Hoe beoordeelt u de omvang van de verwachte lastenverlichting? Mist u aspecten die in de Omnibussen hadden kunnen worden opgenomen die tot verdere besparingen hadden kunnen leiden en in lijn waren geweest met de gestelde doelen?

Antwoord

Ik ben positief over de beoogde lastenverlichting van de omnibussen. In deze raming zijn de effecten van sommige maatregelen niet meegenomen omdat deze moeilijker te kwantificeren zijn. Behalve technische wetswijzigingen vindt het kabinet het ook van belang dat organisaties voldoende praktische ondersteuning krijgen om aan digitale wetgeving te voldoen. Dit is van bijzonder belang omdat digitale wetgeving veelal relatief nieuw is. Hier wordt al aan gewerkt door toezichthouders en de Europese Commissie en de omnibussen geven hier ook

weer een verdere impuls aan door het opstellen van bepaalde richtsnoeren en andere tools te verplichten.

8

De regering plaatst twee kanttekeningen bij de proportionaliteit van de Europese voorstellen. Deze leden achten deze kanttekeningen vrij aanzienlijk en vragen waarom u desondanks positief oordeelt over de proportionaliteit van de Omnibus Digitaal en de Omnibus AI. Verwacht u dat deze aandachtspunten alsnog worden betrokken bij de verdere onderhandelingen?

Antwoord

Voor het oordeel is gekozen omdat het overgrote deel van de voorgestelde wijzigingen proportioneel en positief dan wel aanvaardbaar is. Dat doet er niets aan af dat deze aandachtspunten zwaar wegen voor het kabinet en nadrukkelijk naar voren worden gebracht bij de onderhandelingen.

9

Onlangs heeft de Autoriteit Persoonsgegevens (AP) in een position paper ook haar zorgen geuit over een aantal voorgestelde wijzigingen van de Omnibussen. Zo gaat de drempel omhoog voor het melden van datalekken bij de toezichthouder op grond van de AVG. De Autoriteit Persoonsgegevens (AP) ziet in de praktijk dat organisaties de risico's van een datalek vaak bewust of onbewust onderschatten en geeft hier ook een concreet voorbeeld voor. Deze leden maken zich zorgen dat de autoriteit persoonsgegevens (AP) na de voorgestelde wijziging geen zicht meer heeft op deze gevallen. Deelt u deze zorg van deze leden?

Antwoord

Het kabinet herkent de genoemde zorgen over het voorstel om de meldplicht van datalekken aan de toezichthouder te beperken tot gevallen waarin het datalek een "hoog risico" oplevert voor rechten en vrijheden van betrokkenen. De Autoriteit Persoonsgegevens (AP) heeft in haar Position paper geconstateerd dat verwerkingsverantwoordelijken de risico's van datalekken voor betrokkenen vaak onderschatten.³⁵ De toezichthouder kan verwerkingsverantwoordelijken verplichten om een datalek ook aan betrokkenen te melden (artikel 34, vierde lid, AVG). Door de drempel voor melding aan de toezichthouder, zoals voorgesteld, gelijk te trekken met de drempel voor melding aan betrokkenen, verliezen toezichthouders deze "corrigerende" functie. Dit kan ertoe bijdragen dat personen die door een datalek worden geraakt, daarover niet worden geïnformeerd. Tegelijkertijd steunt het kabinet het doel om het onevenredig hoge aantal meldingen van datalekken aan toezichthouders te verminderen. Daarom stelt het kabinet voor om een middenweg te vinden tussen de drempel in het geldende artikel 33 AVG ("een risico") en de voorgestelde drempel in het voorstel van de Commissie ("hoog risico"). Te denken valt aan "impactvol risico", of eventueel "relevant risico" of "verhoogd risico".

10

³⁵ <https://www.autoriteitpersoonsgegevens.nl/documenten/position-paper-ap-omnibus-digitaal-en-omnibus-ai>

Daarnaast geeft de Autoriteit Persoonsgegevens (AP) in het position paper aan dat de criteria voor de mogelijkheid om het recht op inzage in de AVG te beperken bij 'buitensporige verzoeken' niet duidelijk zijn. Hoe ziet u dit? Hoe beoordeelt u de zorg van de Autoriteit Persoonsgegevens (AP) dat deze onduidelijkheid ertoe zal leiden dat organisaties de term 'buitensporige verzoeken' verschillend zullen uitleggen?

Antwoord

Het kabinet onderschrijft deze kritiek.

Vragen en opmerkingen van de leden van de fractie van PVV

1

De leden van de PVV fractie merken op dat de Omnibus AI voorziet in: *"Het centraliseren van het toezicht door het AI-bureau op een groot aantal AI-systemen die zijn gebaseerd op AI-modellen voor algemene doeleinden of zijn ingebed in zeer grote onlineplatforms en zeer grote zoekmachines"*.

Kunt u aangeven óf en hoe op zo onafhankelijk mogelijke wijze en op gelijkwaardige basis AI-systemen beoordeeld zullen worden door het AI-bureau en op basis van welke concrete criteria?

Antwoord

Het AI-bureau heeft in de huidige AI-verordening al een rol om toezicht te houden op een deel van de AI-modellen voor algemene doeleinden en de AI-systemen die door de aanbieders van dergelijke AI-modellen worden aangeboden. Het AI-bureau zal hier als markttoezichtautoriteit onder dezelfde voorwaarden toezicht op houden als de nationale markttoezichtautoriteiten. De concrete criteria op basis waarvan het AI-bureau toezicht zal houden zijn de eisen aan AI-modellen voor algemene doeleinden en daarop gebaseerde AI-systemen die in de AI-verordening zijn vastgelegd.

2

In het voorstel van de Omnibus AI lezen de leden van de fractie van PVV dat wordt gewerkt aan aanvullende richtsnoeren die gericht zijn op het verstrekken van duidelijke en praktische instructies om de AI-verordening aan andere EU-wetgeving toe te passen. Daarbij gaat het onder meer om: *"richtsnoeren inzake het melden van ernstige incidenten door aanbieders van AI systemen met een hoog risico; richtsnoeren inzake de praktische toepassing van de vereisten met betrekking tot systemen met een hoog risico; richtsnoeren inzake de praktische toepassing van de verplichtingen voor aanbieders en gebruiksverantwoordelijken van AI-systemen met een hoog risico; richtsnoeren met een model voor de effectbeoordeling van de grondrechten."*

Kunt u aangeven wat wordt verstaan onder 'ernstige incidenten', wat daarvoor de omschrijving is, wat de criteria zijn en door wie bepaald wordt wanneer sprake is van een 'ernstig incident'?

Antwoord

In de AI-verordening is een ernstig incident gedefinieerd als:

“ernstig incident”: een incident of gebrekkig functioneren van een AI-systeem dat direct of indirect leidt tot:

- het overlijden van een persoon of ernstige schade voor de gezondheid van een persoon;
- een ernstige en onomkeerbare verstoring van het beheer of de exploitatie van kritieke infrastructuur;
- een schending van de uit het recht van de Unie voortvloeiende verplichtingen ter bescherming van de grondrechten;
- ernstige schade aan eigendommen of het milieu;

Het is in eerste instantie de verantwoordelijkheid van de aanbieder of gebruiksverantwoordelijke om vast te stellen of een dergelijk incident zich heeft voorgedaan. De markttoezichtautoriteiten zullen hierop toezien.

3

Kunt u aangeven wat wordt verstaan onder ‘een hoog risico’, wat daarvoor de omschrijving is, wat de criteria zijn en door wie bepaald wordt wanneer sprake is van een ‘hoog risico’?

Antwoord

Wat hoog risico AI-systemen zijn, is vastgelegd in artikel 6 van de AI-verordening. Hoog risico AI-systemen zijn ten eerste AI-systemen die worden gebruikt als veiligheidscomponent van een product of zelf een product zijn dat onder de harmonisatiewetgeving in bijlage I van de AI-verordening is opgenomen. Dergelijke producten zijn bijvoorbeeld liften of medische hulpmiddelen. Daarnaast worden ook AI-systemen die worden toegepast in een toepassingsgebied dat is opgenomen in bijlage III van de AI-verordening gekwalificeerd als hoog risico. Het gaat daarbij bijvoorbeeld om AI-systemen die worden gebruikt voor emotieherkenning. De aanbieder van het AI-systeem moet in eerste instantie zelf beoordelen of sprake is van een hoog risico AI-systeem. De markttoezichtautoriteiten zullen hier op toezien.

4

Kunt u aangeven hoe in het bijzonder de grondrechten op het gebied van vrijheid van meningsuiting gewaarborgd worden en, óf en hoe, voorkomen wordt dat door maatregelen van de Europese Commissie sprake kan zijn van vormen van censuur?

Antwoord

De (nationale) markttoezichtautoriteiten zullen toezien op het naleven van de grondrechten bij het gebruik van hoog risico AI-systemen, in samenwerking met de grondrechtenautoriteiten. Het gaat hierbij niet om een limitatieve lijst van grondrechten, dus de AI-verordening dient er ook mede toe om het grondrecht op het gebied van vrijheid van meningsuiting te beschermen. In overweging 48 bij de AI-verordening wordt juist onderstreept dat de regels voor AI-systemen met een hoog risico tot doel hebben de grondrechten, waaronder het recht op de vrijheid van meningsuiting, te beschermen.

5

De leden van de PVV-fractie lezen in het voorstel van de Omnibus Digitaal: *"De in deze verordening voorgestelde wijzigingen zullen een centraal toegangspunt invoeren die entiteiten in staat stelt tegelijkertijd aan hun verplichtingen inzake de melding van incidenten uit hoofde van meerdere rechtshandelingen te voldoen. Door het beginsel "eenmalig melden, veelvoudig delen" te bevorderen, zal het centrale toegangspunt de administratieve lasten voor entiteiten verminderen en tegelijkertijd zorgen voor een doeltreffende en veilige informatiestroom over beveiligingsincidenten naar de in de respectieve wetgeving gedefinieerde ontvangers."*

Kunt u nader duiden wat precies wordt verstaan onder een 'centraal toegangspunt' en wat in dit kader bedoeld wordt met 'incidenten' en 'kwetsbaarheden' en hoe en door wie deze bepaald worden?

Antwoord

Met een centraal toegangspunt wordt een Europees meldpunt (single entry point) bedoeld om meldplichten volgend uit verschillende soorten wetgeving, namelijk de Verordening cyberweerbaarheid (CRA), NIS2-richtlijn, CER, DORA, eIDAS en AVG samen te brengen. Deze meldplichten worden nationaal, onder gebruikmaking van verschillende meldpunten, ingericht.

Het kabinet merkt op dat 'incidenten' en 'kwetsbaarheden' in meerdere van de bovenstaande wetgevingen voorkomen. Echter, de passage waar de leden van de PVV-fractie naar verwijzen lijkt te zien op de CRA. In het licht daarvan antwoordt het kabinet als volgt. De CRA richt zich op het verbeteren van digitale producten. Onder deze Verordening moeten de fabrikanten via een centraal meldingsplatform melding doen van actief uitgebuite kwetsbaarheden in producten met digitale elementen en melding doen van ernstige incidenten die gevolgen hebben voor de beveiliging van die producten. De fabrikant zelf is verplicht om te laten controleren of diens product voldoet aan de eisen van de CRA. Eén van deze eisen is dat de fabrikant beveiligingsproblemen – zoals incidenten en kwetsbaarheden – moet kunnen opsporen, melden, oplossen en hierover moet communiceren. In veel gevallen mag de fabrikant zelf een conformiteitsbeoordeling uitvoeren, in andere gevallen moet dit door een externe partij gebeuren.

Vragen en opmerkingen van de leden van de fractie van Volt

1

De regering geeft in de BNC-fiches aan dat impact assessments ontbreken bij de Omnibus Digitaal, de Omnibus AI en de Data Unie Strategie en dat zij hierover bij de Europese Commissie opheldering zou vragen. Heeft u deze opheldering inmiddels gevraagd en gekregen van de Europese Commissie? Als er aanvullende informatie is verstrekt over de impact, bent u dan bereid om die met onze Kamer te delen?

Antwoord

Het kabinet heeft de Europese Commissie verzocht een uitgebreidere analyse van de impact van deze voorstellen te presenteren. Ook brengt het kabinet zelf de gevolgen van de voorstellen verder in kaart. Het lijkt onwaarschijnlijk dat er

alsnog een formeel impact assessment zal worden gepresenteerd. De Commissie heeft wel in de onderhandelingen via onder andere presentaties meer toelichting gegeven. Deze documenten zijn als onderdeel van de onderhandelingen vertrouwelijk en kan ik daarom niet met uw Kamer delen. Middels onder andere deze beantwoording deel ik wel zoveel mogelijk nieuwe informatie met uw Kamer, binnen de ruimte die daarvoor is gezien de informatie-afspraken binnen de Raad en de vertrouwelijkheid van onderhandelingsstukken.

2

De regering geeft in het BNC-fiche aan dat het ontbreken van de impact assessment het voor de regering moeilijk maakt om te beoordelen welke effecten de Omnibus Digitaal en de Omnibus AI zullen hebben op de verlaging van de regeldruk en op de fundamentele grondrechten en de nationale bevoegdheden. Bent u van mening dat de voorgestelde wijzigingen en de afwegingen die de Europese Commissie daarbij heeft gemaakt voldoende kunnen worden beoordeeld? Zo nee, van welke voorgestelde wijzigingen kunt u nu de impact op de fundamentele rechten of de doelmatigheid (nog) niet goed inschatten of afwegen?

Antwoord

Op basis van het voorstel zelf en het bijgaande SWD is het moeilijk om de effecten te beoordelen van de voorstellen die verdergaan dan het versimpelen, verduidelijken en stroomlijnen van wetgeving. Dit geldt met name voor wijzigingen aan de AVG die afbreuk doen aan de het niveau van gegevensbescherming, zoals toegelicht in het BNC-fiche. Voor de beoordeling van de impact van de voorstellen hecht het kabinet zeer aan de gezamenlijke adviezen van de EDPB en de EDPS. Deze adviezen bestudeert het kabinet momenteel. Voor een aantal voorgestelde wijzigingen aan de AVG, waaronder het wijzigen van de definitie van persoonsgegevens, lijkt er wel steun van een aantal lidstaten om deze wijzigingen terug te draaien of zo aan te passen dat de impact van de wijzigingen op grondrechten wordt geminimaliseerd. Zoals aangegeven in deze beantwoording lijkt er onder andere voldoende steun van verschillende lidstaten om het wijzigen van de definitie van persoonsgegevens terug te draaien. Als dit de Raadspositie zou worden zou dit geen impact hebben op fundamentele rechten.

Voor zover voorgestelde wijzigingen komen te vervallen, zou de noodzaak komen te ontvallen aan het verrichten van een impact assessment voor de betreffende wijzigingen.

3

Wanneer verwacht u de nog ontbrekende informatie over de impact van de verschillende wijzigingen bij de Europese Commissie te kunnen opvragen? Kunt u een aanvullende impactbeoordeling delen met onze Kamer?

Antwoord

Zoals aangegeven in de beantwoording van de eerste vraag van de leden van uw fractie zijn de documenten die de Europese Commissie als onderdeel van de onderhandelingen deelt vertrouwelijk en kan ik deze niet met uw Kamer delen. Middels onder andere deze beantwoording deel ik wel zoveel mogelijk nieuwe

informatie met uw Kamer, binnen de ruimte die daarvoor is gezien de informatie-afspraken binnen de Raad en de vertrouwelijkheid van onderhandelingsstukken.

4

De leden van de Volt-fractie lezen in het BNC-fiche dat de regering een risico ziet op meer politieke besluitvorming bij de uitvoering van de AVG, omdat de Omnibus Digitaal uitvoeringsbevoegdheden verschuift van de onafhankelijke nationale en Europese toezichthouder(s) naar de Europese Commissie. Wat zal de verdere inzet van de regering zijn met betrekking tot dit risico bij de behandeling van de Omnibus Digitaal? Denkt u dit risico te kunnen mitigeren? Zo ja, op welke wijze?

Antwoord

Het kabinet brengt de zorgen over de verschuiving van bevoegdheden naar de Europese Commissie – zoals omschreven in het BNC-fiche – naar voren tijdens de onderhandelingen. Het kabinet voelt zich hierin onder meer gesterkt door het advies van de EDPB en EDPS van 10 februari jl., die hebben aanbevolen om de Commissie geen rol te geven bij de vaststelling van de lijsten over wanneer DPIA's of meldingen van datalekken verplicht zijn, en ook niet bij criteria inzake pseudonimisering. Er lijkt voldoende steun in de Raad om deze bevoegdheden voor de EDPB te behouden.

5

De regering geeft in het BNC-fiche aan dat zij de adviezen van de Europees Toezichthouder voor gegevensbescherming (EDPS) en van het Europees Comité voor gegevensbescherming (EDPB) wil betrekken bij haar beoordeling en inzet op de Omnibus Digitaal en de Omnibus AI. Deze adviezen zijn inmiddels verschenen. Kunt u aangeven of u de adviezen en de daarin geuite zorgen onderschrijft? Hoe zal de regering deze adviezen bij de verdere Nederlandse inzet betrekken?

Antwoord

In de gezamenlijke EDPB/EDPS-opinie over de Omnibus Digitaal zijn de EDPB en EDPS kritisch over de impact van de voorgestelde wijzigingen op het niveau van bescherming van de grondrechten op privacy en gegevensbescherming. De opinie komt op delen overeen met het standpunt dat het kabinet ten aanzien van de Omnibus Digitaal en het kabinet ziet het dan ook als steun voor die positie. Het kabinet betreft de adviezen bij de verdere Nederlandse inzet, onder meer doordat Nederland aan het voorzitterschap van de Raad heeft gevraagd om de voorzitters van de EDPB en EDPS uit te nodigen om een presentatie te houden in het gremium waarin de onderhandelingen worden gevoerd, de Antici Group on Simplification. Die presentatie, met vraag en antwoord sessie, is gehouden op 27 februari jl.

6

De regering geeft in het BNC-fiche aan grote zorgen te hebben over het instellen van een Europees meldpunt. Hoe meent u bij de behandeling van de Omnibus Digitaal te kunnen bereiken dat in plaats daarvan wordt voortgeborduurd op nationale meldpunten en oplossingen, zoals de regering in het BNC-fiche voorstaat?

Antwoord

Het kabinet benadrukt dat nationale meldstructuren, waarbij instanties van lidstaten de directe ontvanger van incidentinformatie zijn, behouden moet blijven. Het kabinet is van mening dat het verlagen van de regeldruk meer efficiënt en tijdig kan worden bereikt door voort te bouwen op juist deze nationale structuren en dat er op nationaal niveau nog veel ruimte is voor doorontwikkeling en harmonisatie, waarbij EU-breed optreden niet nodig is. Het kabinet zal tijdens de onderhandelingen de meerwaarde van de nationale meldstructuren blijven benadrukken en in overleg treden met lidstaten met vergelijkbare posities. Hoewel het kabinet zorgen heeft over de inrichting Europees meldpunt, onderschrijft het de doelstelling om de regeldruk voor bedrijven te verminderen. Het kabinet zal zich dan ook inzetten voor de harmonisatie van de cybersecuritywetgeving door concrete voorstellen te formuleren.

7

De Omnibus Digitaal voorziet in een wijziging van de definitie van "persoonsgegevens". Onderschrijft u dat de voorgestelde wijziging leidt tot subjectiviteit en (rechts)onzekerheid met betrekking tot wanneer sprake is van persoonsgegevens en wanneer de AVG van toepassing is?

Antwoord

Ja, zoals toegelicht in de beantwoording van vraag 57 van de leden van de fractie van GL/PvdA.

8

EDPB en EDPS uiten zorgen over het verruimen van het gebruik van bijzondere persoonsgegevens over bijvoorbeeld etniciteit of gezondheid voor het opsporen en corrigeren van discriminatie in AI-systemen. Deelt u de opvatting van de Europese Commissie dat de bescherming tegen het gebruik van die gegevens in het huidige AI-landschap kan worden versoepeld? Zo ja, op basis waarvan komt u tot die conclusie? Wordt het risico op herleidbaarheid niet juist groter naarmate AI zich verder ontwikkelt, en blijft de bescherming daarom niet onverminderd noodzakelijk om directe of indirecte discriminatie te voorkomen? Op welke aanvullende waarborgen zet u in bij de verdere behandeling van de Omnibus Digitaal?

Antwoord

Eenzijds leidt deze aanpassing tot een mogelijke verbetering van het recht op non-discriminatie, omdat er meer AI-systemen aan een grondigere bias-controle en -correctie onderworpen kunnen worden. Anderzijds kan verkeerd gebruik van deze mogelijkheid leiden tot inbreuken op het recht op gegevensbescherming. Daarom pleit het kabinet tijdens de onderhandelingen voor duidelijke waarborgen en een strikte noodzakelijkheid.

9

De Omnibus AI voorziet in het schrappen van de registratieplicht voor AI-systemen die aanbieders zelf niet aanmerken als hoog risico. Bent u bekend met de bezwaren die de toezichthouders AP en de EDPB hiertegen hebben geuit?³⁴ Deelt u de opvatting dat het schrappen van deze registratieplicht de transparantie

en de uitvoerbaarheid van het toezicht vermindert? Op welke wijze betreft u de zorgen van de toezichthoudende instanties bij de verdere Nederlandse inzet ten aanzien van de Omnibus Digitaal en de Omnibus AI?

Antwoord

Voor de kabinetspositie ten opzichte van het omnibusvoorstel om de registratieplicht voor AI-systemen die beoordeeld zijn als niet hoog risico door de aanbieder, verwijs ik u naar het antwoord op vragen 38 tot en met 43 van GroenLinks/PvdA.

10

In het BNC-fiche heeft de regering zorgen geuit over de grondslag die in de Omnibus Digitaal wordt geïntroduceerd voor het verwerken van (bijzondere) persoonsgegevens. De regering geeft aan dat het belangrijk is dat er goede randvoorwaarden zijn. Welke randvoorwaarden moeten volgens u aanwezig zijn? Hoe zet de regering zich bij de behandeling van de Omnibus Digitaal in voor die randvoorwaarden?

Antwoord

Wanneer bijzondere persoonsgegevens mogen worden verwerkt is het extra belangrijk dat er goede randvoorwaarden zijn gezien de gevoeligheid van bijzondere categorieën persoonsgegevens. Of er een uitzondering op het verbod om bijzondere persoonsgegevens te verwerken moet worden gemaakt in het kader van de ontwikkeling en exploitatie van een AI-systeem of AI-model, vergt nadere beoordeling. Dit zou alleen aan de orde kunnen zijn als de fundamentele rechten voldoende gewaarborgd zijn. De voorgestelde uitzondering mag de bescherming van bijzondere persoonsgegevens niet ondermijnen. Van het verbod op de verwerking van bijzondere categorieën van persoonsgegevens mag uitsluitend worden afgeweken, indien er passende waarborgen worden geboden ter bescherming van persoonsgegevens en andere grondrechten, gelet op de significante risico's die verwerking kan meebrengen voor de grondrechten en de fundamentele vrijheden (zie overweging 51 en 52 AVG). Het kabinet is daarom kritisch op het voorgestelde artikel 9, tweede lid, onder k. Hierin wordt namelijk onder meer bepaald dat bijzondere persoonsgegevens niet hoeven te worden verwijderd "indien de verwijdering van die gegevens onevenredig veel moeite vergt". Dit draait de gedachte achter het gegevensbeschermingsrecht om omdat het, naarmate er meer persoonsgegevens worden verwerkt, makkelijker zou worden om te rechtvaardigen dat bijzondere persoonsgegevens mogen worden verwerkt. Voorkomen moet worden dat verwerkingsverantwoordelijken standaard een onevenredige inspanning zouden kunnen claimen als het om grote of ongestructureerde datasets gaat. Bovendien gaat dit voorstel voorbij aan het techniekneutrale karakter van de AVG. Voorkomen moet worden dat verwerkingsverantwoordelijken onnodig AI zouden gaan gebruiken, vanwege het enkele feit dat zij dan met behulp van de voorgestelde uitzondering kunnen stellen over ruimere gegevensverwerkingsmogelijkheden te beschikken. Voorkomen moet daarom worden dat bijzondere persoonsgegevens die via een AI-systeem of -model worden verwerkt, gunstiger worden behandeld dan via een andere, gebruikelijke verwerkingsmethode.

11

De leden van de fractie van Volt constateren dat de regering een positieve houding inneemt ten aanzien van het voorstel van gecentraliseerde cookie-toestemming in de Omnibus Digitaal (art. 88ter). Voor digitale 'gatekeepers' onder de Digitale Markets Act (DMA) is dit begrijpelijk. Tegelijkertijd kan dit voorstel negatieve gevolgen hebben voor nieuwsuitgevers op de online advertentiemarkt en ook voor media dienstverleners. Op welke wijze wordt dit meegenomen bij de Nederlandse inzet? Bent u bereid voor beide een uitzonderingspositie te bedingen? In hoeverre acht u het risico aanwezig dat gecentraliseerde cookie-toestemming een oneigenlijk voordeel voor bepaalde delen van de digitale markt ten opzichte van andere delen daarvan?

Antwoord

Hiervoor verwijs ik u naar de beantwoording van vragen 92 en 93 van de leden van de fractie van GL/PvdA.

Vragen en opmerkingen van het lid van fractie-Van de Sanden

1

Kunt u uiteenzetten hoe u voorkomt dat de Omnibus Digitaal leidt tot een verdere verschuiving van bevoegdheden van nationale naar Europese toezichthouders zonder adequate democratische controle? Welke concrete waarborgen worden ingebouwd om te verzekeren dat de rol van nationale parlementen niet wordt gemarginaliseerd?

Antwoord

De omnibus verandert in principe weinig aan de rol van nationale parlementen. Met het voorgestelde Europees meldpunt verschuift een deel van de nationale dienstverlening rondom incidentenafhandeling naar Europees niveau. Het kabinet zal tijdens de onderhandelingen de meerwaarde van de nationale meldstructuren blijven benadrukken en in overleg treden met lidstaten die vergelijkbare posities innemen. Nationale meldstructuren en meldpunten sluiten aan bij de manier van samenwerken en communiceren die entiteiten hebben met de Nederlandse overheid. Het kabinet verwacht dat het verlagen van regeldruk meer efficiënt en tijdig kan worden bereikt door voort te bouwen op bestaande nationale oplossingen in plaats van het organiseren van een Europees meldpunt.

2

Welke proportionaliteitstoets heeft u uitgevoerd met betrekking tot de afzonderlijke onderdelen van de Omnibus Digitaal en de Omnibus AI? Kunt u per voorgestelde maatregel aangeven waarom deze noodzakelijk is, welk probleem wordt opgelost en waarom een minder ingrijpend alternatief niet volstaat?

Antwoord

Het kabinet heeft de voorstellen zoals gebruikelijk getoetst op proportionaliteit. In het BNC-fiche is hier ook een oordeel over gegeven. Veel van de voorgestelde wetwijzigingen betreffen verduidelijkingen en versimpelingen van bestaande EU-wetgeving die weinig tot geen effect hebben behalve het verlagen van regeldruk. Deze wijzigingen zie het kabinet als proportioneel omdat deze niet verder gaan

dan noodzakelijk. De aanpassingen doen geen afbreuk doen aan de beoogde doelen en werking van de wetgeving.

Zoals aangegeven in het BNC-fiche heeft het kabinet ook vragen en zorgen over de proportionaliteit van een aantal voorgestelde wijzigingen en zet het in de onderhandelingen in op minder ingrijpende alternatieven. Dit gaat over een aantal voorgestelde wijzigingen aan de AVG die verder lijken te gaan dan noodzakelijk door het niveau van gegevensbescherming verminderen. Het is bovendien onduidelijk of deze wijzigingen de regeldruk wel verlagen. Met betrekking tot het Europees meldpunt vindt het kabinet dat ook dat onvoldoende inzichtelijk is gemaakt of dit meldpunt leidt tot lastenverlichting, terwijl het meldpunt wel o.a. beveiligingsrisico's en risico's met betrekking tot de afhankelijkheid van een platform dat op EU niveau wordt beheerd zich mee brengt. Tot slot ziet het kabinet dat het volledig intrekken van de P2B-verordening mogelijk ingrijpender is dan nodig omdat dit afbreuk doet aan het niveau van bescherming van ondernemers op online platforms. Door bepaalde bepalingen uit de P2B-verordening in stand te houden kan de regeldruk worden verlaagd zonder de bescherming van ondernemers op online platforms te verzwakken.

3

Op welke wijze heeft u in kaart gebracht welke administratieve lastenreductie de Omnibus Digitaal daadwerkelijk oplevert voor Nederlandse bedrijven, in het bijzonder voor het midden- en kleinbedrijf en start-ups? Kunt u een concrete kosten-batenanalyse delen?

Antwoord

Een concrete kosten-baten analyse voor de Nederlandse situatie wordt niet voorzien. Dit wordt ook bemoeilijkt omdat het voorstel gezien het tempo van de onderhandelingen voortdurend aan verandering onderhevig is. Het kabinet heeft de Europese Commissie verzocht uitgebreidere analyse van de impact van de voorstellen te presenteren en brengt zelf de gevolgen van de voorstellen verder in kaart.

4

Hoe waarborgt u dat de aanpassingen in de Omnibus AI, waaronder uitstel van bepaalde verplichtingen uit de AI-verordening, niet leiden tot een verzwakking van de bescherming van fundamentele rechten zoals privacy, gelijke behandeling en het recht op effectieve rechtsbescherming?

Antwoord

Het kabinet acht het van belang dat de doelen van de AI-verordening overeind blijven, zoals ook is benadrukt in het BNC-fiche. Per voorstel uit de Omnibus AI heeft het kabinet beoordeeld in hoeverre dit het geval is.

5

In hoeverre beperken deze voorstellen de ruimte voor Nederland om eigen keuzes te maken op het terrein van digitalisering en AI-toepassingen? Kunt u aangeven welke onderdelen leiden tot volledige harmonisatie en waar nog nationale beleidsvrijheid resteert?

Antwoord

De voorgestelde wijzigingen aan bestaande wetgeving veranderen weinig aan de beleidsvrijheid van lidstaten en veranderen niet de mate van harmonisatie van de onderliggende wetgeving. De enige concrete zorg op dit vlak is, zoals toegelicht in het BNC-fiche, dat het voorgestelde Europees meldpunt een deel van de nationale dienstverlening rondom incidentenafhandeling verschuift naar Europees niveau. Het kabinet benadrukt op dit punt dat nationale meldstructuren, waarbij lidstaten de directe en primaire ontvanger van incidentinformatie blijven, behouden moeten blijven.

6

Welke mogelijkheden blijven voor burgers en bedrijven bestaan om besluiten van Europese digitale toezichthouders aan te vechten bij een onafhankelijke rechter? Acht u deze rechtsbescherming toereikend. Zo ja, op grond waarvan?

Antwoord

De voorstellen voor de omnibussen veranderen niets aan de mogelijkheden voor burgers en bedrijven om besluiten van (Europese) digitale toezichthouders aan te vechten bij een onafhankelijke rechter.

7

De regering plaatst in het BNC-fiche een kanttekening bij het voorgestelde Europese meldpunt voor rapportageverplichtingen. Kunt u nader toelichten waarom desondanks geen formeel subsidiariteitsbezwaar wordt overwogen? Welke meerwaarde ziet u in dit meldpunt ten opzichte van nationale voorzieningen?

Antwoord

Met betrekking tot de meerwaarde reageert het kabinet als volgt. De meerwaarde van een Europees meldpunt ten opzichte van nationale voorzieningen is volgens het kabinet (nog) niet toereikend gemotiveerd. Door de Commissie is nog onvoldoende inzichtelijk gemaakt of een dergelijk meldpunt daadwerkelijk zorgt voor lastenverlichting en simplificatie ten opzichte van de nationale meldstructuur. In het bijzonder waar het gaat om niet-grensoverschrijdende entiteiten. Het kabinet zet zich ervoor in om hierin meer inzicht te krijgen om zo te kunnen beoordelen of dit onderdeel de subsidiariteitstoets kan doorstaan.

8

Hoe beoordeelt u de risico's dat de stapeling van Europese digitale regelgeving – waaronder de Omnibus Digitaal en de Omnibus AI – het Nederlandse innovatieklimaat kan verzwakken? Welke concrete maatregelen neemt u om te voorkomen dat compliance-eisen innovatie ontmoedigen?

Antwoord

De Omnibus Digitaal en de Omnibus AI beogen juist de regeldruk van digitale wetgeving te verlagen. Daarmee dragen ze positief bij aan het innovatieklimaat. Het verlagen van regeldruk is ook voor het kabinet een belangrijke prioriteit en het kabinet ziet net als de Europese Commissie dat dit kan bijdragen aan het versterken van het innovatie- en concurrentievermogen. Over de omnibussen als

geheel verwacht het kabinet dat de omnibussen inderdaad de regeldruk verlagen en daarmee bijdragen aan het versterken van het concurrentievermogen.

9

Hoe verhouden de voorstellen zich tot het streven naar behoud van Nederlandse en Europese digitale soevereiniteit? Kunt u aangeven op welke punten strategische beslissingsmacht feitelijk uit nationale handen wordt overgedragen en hoe dit wordt gewogen?

Antwoord

Het kabinet ziet net als de Europese Commissie dat het verlagen van regeldruk kan bijdragen aan het versterken van het innovatie- en concurrentievermogen. Over de omnibussen als geheel verwacht het kabinet dat de omnibussen inderdaad de regeldruk verlagen en daarmee bijdragen aan het versterken van het concurrentievermogen.

De omnibussen dragen geen strategische beslissingsmacht van nationale overheden over naar EU-niveau. Zoals aangegeven in het antwoord op vraag 5 van uw fractie aangegeven verschuift het voorgestelde Europees meldpunt wel een deel van de nationale dienstverlening rondom incidentenafhandeling verschuift naar Europees niveau. Het kabinet benadrukt op dit punt dat nationale meldstructuren, waarbij lidstaten de directe en primaire ontvanger van incidentinformatie blijven, behouden moeten blijven.

Willemijn Aerdt

Staatssecretaris van Economische Zaken - Digitale Economie en Soevereiniteit

Directoraat-generaal
Economie en Digitalisering

Aan de Staatssecretaris Digitale Economie en Soevereiniteit

Auteur
[Redacted]
[Redacted]
[Redacted]

TER BESLISSING
Datum aangemaakt
6 maart 2026

Kenmerk
DGED / 104522581

Kopie aan
[Redacted]

Bijlage(n)
1

nota
TER BESLISSING

Beantwoording Eerste Kamervragen Omnibus AI,
Omnibus Digitaal en Data Unie Strategie

Parafenroute
[Redacted] [Redacted] [Redacted]
[Redacted] [Redacted] [Redacted]
[Redacted]
[Redacted]

**ligt parallel bij DG/SEZ*

Aanleiding

De leden van de Eerste Kamerfracties van GroenLinks-PvdA, BBB, D66, PvdD, PVV, Volt en fractie-Van de Sanden hebben schriftelijke vragen gesteld naar aanleiding van de voorstellen voor de Omnibus Digitaal, Omnibus AI en de Data Unie Strategie, evenals de bijbehorende BNC-fiches.

Geadviseerd besluit

Bijgevoegde beantwoording op de vragen van de leden van de Eerste Kamer ondertekenen en instemmen met het verzenden ervan aan de Eerste Kamer.

Kernpunten

- Gelijktijdig met de vragen heeft de Eerste Kamer ook een brief verzonden waarmee ze een parlementair behandelvoorbehoud inroept op de Omnibus AI en de Omnibus Digitaal. 17 maart zal daarom een mondeling overleg met de Eerste Kamer plaatsvinden over de digitale omnibussen. De Eerste Kamer verzoekt deze beantwoording daarom uiterlijk 13 maart te verzenden.
- De vragen gaan veelal over dezelfde onderwerpen als waar de Tweede Kamer eerder vragen over heeft gesteld. De fracties stellen veelal kritische vragen over de onderdelen van de omnibussen waar het kabinet zich in het BNC-fiche over de beide Omnibussen ook kritisch over heeft geuit. Veel vragen gaan over de gevolgen van de voorstellen, de manier waarop het kabinet haar inzet gaat bewerkstelligen, of er steun is voor de inzet bij andere lidstaten en of het kabinet haar steun voorwaardelijk maakt aan bepaalde concrete aanpassingen.
- De beantwoording is in lijn met de eerdere beantwoording van de Tweede Kamervragen over de omnibussen. De beantwoording geeft aan dat voor een aantal belangrijke zorgpunten van het kabinet steun lijkt te zijn van verschillende lidstaten om deze zorgen te adresseren. Dit gaat o.a. om de zorgen over het Europees centraal meldpunt, het schrappen van de

registratieplicht voor bepaalde hoog-risico AI-systemen en het wijzigen van de definitie van persoonsgegevens.

Kenmerk
DGED / 104522581

- In de beantwoording wordt ook aangegeven dat het kabinet zich in eerste instantie inzet om via de onderhandelingen het voorstel in lijn met haar inzet te verbeteren. Het kabinet zal op basis van het uiteindelijk onderhandelingsresultaat beoordelen of het resultaat voldoende in lijn is met de Nederlandse inzet.
- Via deze beantwoording geeft u ook alvast aan welke informatie-afspraken u met de Eerste Kamer zou willen maken. Het voorstel is om aan te sluiten bij de informatie-afspraken die zijn gemaakt met de Tweede Kamer. Dat houdt in dat de reguliere informatievoorziening primair zal plaatsvinden via de geannoteerde agenda's voor de Telecomraden. Waar nodig zullen aanvullende Kamerstukken worden verstuurd, bijvoorbeeld over substantiële veranderingen aan de omnibussen en wanneer er een akkoord of definitieve compromistekst ligt.
- Twee thema's komen zeer regelmatig terug in de vragen:
 - **Zorgen over fundamentele aanpassingen aan de AVG** die de bescherming van de grondrechten privacy en gegevensbescherming aantasten. In de beantwoording wordt aangegeven dat het kabinet deze zorgen deelt. Het kabinet zet erop in dat deze onderdelen van de omnibussen worden behandeld op een manier die recht doet aan deze zorgen. De risico's en impact van de voorstellen moeten helder zijn voordat het kabinet een oordeel kan geven over de effectiviteit en wenselijkheid van de voorstellen. Daarnaast zet het kabinet erop in de inhoudelijke zorgen te adresseren in de lopende onderhandelingen.
 - **Hoe de impact van de voorstellen wordt beoordeeld** bij gebrek aan een formeel impact assessment voor de voorstellen. In de beantwoording wordt aangegeven dat voor de voorstellen die zich in lijn met de kabinetsinzet focussen op versimpelen, verduidelijken en stroomlijnen van wetgeving de door de Commissie gepresenteerde informatie voldoende basis biedt voor onderhandelingen. Voor sommige voorstellen die verdergaan dan versimpeling maakt het ontbreken van een impact assessment het initieel moeilijk de effecten te beoordelen. Het kabinet heeft de Europese Commissie verzocht een uitgebreidere analyse van de impact van deze voorstellen te presenteren en onderzoekt zelf de impact van deze voorstellen.



Eerste Kamer der Staten-Generaal

Staatssecretaris Digitale Economie en Soevereiniteit
Mevrouw mr. drs. W.J.M. Aerdts
Postbus 20401
2500 EK Den Haag

Kazernestraat 52
2514 CV Den Haag
postbus 20017
2500 EA Den Haag

telefoon 070 312 92 00
fax 070 312 93 90

e-mail postbus@eerstekamer.nl
internet www.eerstekamer.nl

datum 24 februari 2026

betreft Omnibus Digitaal, Omnibus AI en Data Unie Strategie

ons kenmerk 179856

Geachte mevrouw Aerdts,

De vaste commissies voor Digitalisering en Economische Zaken & Klimaat en Groene Groei hebben met belangstelling kennisgenomen van de voorstellen van de Europese Commissie: Omnibus Digitaal (COM(2025)837), Omnibus AI (COM(2025)836) en de Data Unie Strategie (COM(2025)835). Naar aanleiding van deze voorstellen en de hierbij horende BNC-fiches wensen de leden van de fracties van **GroenLinks-PvdA**, **BBB**, **D66**, mede namens de leden van de fractie van de **PvdD**, **PVV**, **Volt** en **fractie-Van de Sanden** enkele vragen te stellen aan u.

1. Vragen van de leden van de fractie van GroenLinks-PvdA

De leden van de fractie van **GroenLinks-PvdA** hebben kennisgenomen van het BNC-fiche voor de Omnibus Digitaal en de Omnibus AI en het BNC-fiche voor de Data Unie Strategie. Zij delen de zorgen van de regering over de voorliggende voorstellen. Deze leden hebben hierover enkele vragen en opmerkingen.

a. Algemene vragen

De leden van de fractie van GroenLinks-PvdA merken op dat er geen integrale *impact assessment* is gemaakt van Omnibus Digitaal, de Omnibus AI en de Data Unie Strategie. Dat vinden deze leden zeer zorgelijk. In het BNC-fiche lezen deze leden dat ook de regering hier zorgen over heeft. De leden merken op dat een *impact assessment* vereist is voor Europese voorstellen die mogelijk significante economische, ecologische of sociale gevolgen hebben. Dit geldt voor zowel wetgevingsvoorstellen (richtlijnen/verordeningen) als belangrijke niet-wetgevingsinitiatieven (zoals mededelingen of actieplannen). Een *impact assessment* is onderdeel van de agenda "*Better Regulation*" (betere regelgeving) van de Europese Commissie.

1. Deelt u de conclusie van deze leden dat een integrale *impact assessment* een verplicht onderdeel is? Zo nee, waarom niet? Zo ja, wat betekent deze verplichting voor de kabinetsinzet? Is dit een harde voorwaarde om te kunnen starten met de onderhandelingen en/of in te kunnen stemmen met de voorstellen? Deze leden ontvangen graag een toelichting.



datum 24 februari 2026

ons kenmerk 179856

blad 2

De leden van de fractie van GroenLinks-PvdA merken op dat als de Europese Commissie bij een voorstel voor een verordening geen *impact assessment* maakt, lidstaten en andere actoren verschillende politieke en juridische mogelijkheden hebben om de Europese Commissie hiertoe aan te sporen. Verordeningen zijn rechtstreeks van toepassing in lidstaten en hebben dus directe werking, waardoor actie tijdens het wetgevingsproces cruciaal is.

2. Welke mogelijkheden ziet u om tijdig een integrale *impact assessment* beschikbaar te krijgen? Deze leden ontvangen hier graag een volledige opsomming van.
3. Welke mogelijkheden bent u voornemens om in te zetten?
4. Ziet u kansen om hierbij allianties met andere landen te vormen? Deze leden ontvangen graag een toelichting.
5. Ziet u kansen om hierbij een beroep te doen op het Interinstitutioneel Akkoord Beter Wetgeven? Deze leden ontvangen graag een toelichting.
6. Hoe verhouden de Data Unie strategie, de Omnibus Digitaal en de Omnibus AI zich tot de doelstellingen van de Nationale Digitalisering Strategie? Deze leden ontvangen graag een toelichting.
7. Welke wet- en regelgeving wordt door deze aanpassingen geraakt, direct dan wel indirect? Worden de Wet politiegegevens en de Wet justitiële en strafvorderlijke gegevens bijvoorbeeld geraakt?
8. Welke uitvoeringsorganisaties worden geraakt door deze aanpassingen? Deze leden ontvangen graag een toelichting.
9. Zijn deze uitvoeringsorganisaties geconsulteerd over de effecten die zijn voorzien voor de eigen organisatie en de gebruikers (burgers en bedrijven), en wat was hun visie/oordeel? Deze leden ontvangen graag een toelichting per uitvoeringsorganisatie.

De leden van de fractie van GroenLinks-PvdA merken op dat de geopolitieke situatie aan grote veranderingen onderhevig is. In de huidige geopolitieke situatie is Nederlandse/Europese (digitale) autonomie een belangrijk speerpunt. Een agenda van deregulering, zoals de Omnibussen, met het oog op de vrije digitale markt, is in het voordeel van de grote (Amerikaanse) techbedrijven, zo menen de leden van de fractie van GroenLinks-PvdA. Wellicht vraagt de huidige situatie juist een tegengestelde beweging, namelijk van gerichtere (digitale) regulering in plaats van deregulering.

10. Hoe beoordeelt u de Omnibus Digitaal, de Omnibus AI en de Data Unie Strategie in de huidige geopolitieke situatie? Deze leden ontvangen graag een toelichting.

b. Grondrechten in het geding

De leden van de fractie van GroenLinks-PvdA merken op dat het College voor de Rechten van de Mens is vastgesteld als grondrechtenautoriteit Artificiële Intelligentie (AI) in Nederland.¹ De Omnibus Digitaal vormt volgens het College "een zorgwekkende ontwikkeling voor de bescherming van grondrechten, zoals het recht op non-discriminatie en gegevensbescherming".²

¹ College voor de Rechten van de Mens, 'College wordt grondrechtentoezichthouder Artificiële Intelligentie', 20 november 2024, <https://www.mensenrechten.nl/actueel/nieuws/2024/11/15/college-wordt-grondrechtentoezichthouder-artificiele-intelligentie>.

² College voor de Rechten van de Mens, 'EU-wetswijzingen 'digitale omnibus' zorgelijk voor grondrechten', 19 november 2025, <https://www.mensenrechten.nl/actueel/nieuws/2025/11/19/eu-wetswijzingen-digitale-omnibus-zorgelijk-voor-grondrechten>.



datum 24 februari 2026

ons kenmerk 179856

blad 3

11. Kunt u een inhoudelijke reactie geven op deze uitspraak van het College voor de Rechten van de Mens?
12. Kunt u een overzicht geven van alle potentiële aantastingen van grondrechten (uit de Nederlandse Grondwet en Europese wetgeving) die in het geding zijn? Kunt u deze uiteenzetting duidelijk relateren aan de voorgestelde wijzigingen? Deze leden verzoeken u hierbij speciale aandacht te besteden aan artikel 8 van het Handvest van de grondrechten van de Europese Unie.

c. Ondernemingsklimaat

De leden van de fractie van GroenLinks-PvdA merken op dat er niet één allesomvattend optimaal ondernemingsklimaat bestaat dat voor alle typen bedrijven even gunstig is.

13. Ziet u een spanningsveld tussen de belangen van het Midden- en Kleinbedrijf (MKB) in Nederland en Europa enerzijds en grote (Amerikaanse) techbedrijven anderzijds in deze voorstellen? In hoeverre worden grote spelers bevoordeeld ten opzichte van het MKB? Deze leden ontvangen graag een toelichting.
14. Bent u van mening dat de Digitale Omnibus, de Omnibus AI en de Data Unie Strategie eerlijke concurrentie waarborgen? Of wordt er een rode loper uitgelegd voor de verdienmodellen van grote (Amerikaanse) techbedrijven ten koste van de privacy? Deze leden ontvangen graag een toelichting.
15. Ziet u mogelijk nog andere effecten die voor verschillende groepen ondernemers anders uitwerken? Deze leden ontvangen graag een toelichting.
16. European Digital Rights (EDRI) stelt dat de 'vereenvoudiging' nieuwe complexiteit introduceert en dat grote bedrijven de juridische afdelingen hebben om deze mazen in de wet op te zoeken, terwijl het MKB in onzekerheid achterblijft.³ Kunt u hierop reflecteren?

De leden van de fractie van GroenLinks-PvdA lezen dat grote techbedrijven ruim 150 miljoen per jaar uitgeven aan de lobby voor hun belangen in Europa.⁴

17. Heeft u zicht op deze lobby? Hoe beoordeelt u de invloed van deze lobby, waarbij vertraging, versoepeling en herformulering een belangrijke rol speelt bij de totstandkoming van de voorstellen? Deze leden ontvangen graag een toelichting.

De leden van de fractie van GroenLinks-PvdA lezen dat Corporate Europe Observatory de invloed van de lobby van grote (Amerikaanse) techbedrijven op verschillende artikelen van de Omnibus Digitaal heeft geanalyseerd.⁵

18. Kunt u reflecteren op de analyse van Corporate Europe Observatory?

³ ICS, 'The Digital Omnibus: Simplifying Europe's Digital Rulebook and Its Impact on Ireland', 26 november 2025, <https://ics.ie/2025/11/26/the-digital-omnibus-simplifying-europes-digital-rulebook-and-its-impact-on-ireland/>.

⁴ Digwatch, 'Big Tech ramps up Brussels lobbying as EU considers easing digital rules', 30 oktober 2025, <https://dig.watch/updates/big-tech-ramps-up-brussels-lobbying-as-eu-considers-easing-digital-rules#:~:text=Spending%20is%20concentrated%20among%20US,so%2C%20ask%20our%20Diplo%20chatbot>

⁵ Corporate Europe Observatory, 'Article by article, how Big Tech shaped the EU's roll-back of digital rights', 14 januari 2026, <https://corporateeurope.org/en/2026/01/article-article-how-big-tech-shaped-eus-roll-back-digital-rights>.



datum 24 februari 2026

ons kenmerk 179856

blad 4

19. In het kader van transparantie is het belangrijk om ook zicht te hebben op de lobby in Nederland. Welke contacten heeft de Nederlandse regering en/of de ambtelijke ondersteuning gehad met lobbyisten van techbedrijven om de standpunten te bepalen? Deze leden ontvangen graag een toelichting.

d. Wijzigingen bevoegdheden

De leden van de fractie van GroenLinks-PvdA wijzen erop dat de in de Omnibus Digitaal voorgestelde bevoegdheden voor de Europese Commissie om op grond van de AVG een aantal uitvoeringshandelingen vast te stellen, leidt tot een verschuiving van bevoegdheden van de onafhankelijke toezichthouders en de EDPB naar de Europese Commissie. Het betreft bevoegdheden voor de Europese Commissie om standaarden voor datalekmeldingen en omschrijving van hoog risico gevallen voor datalekken vast te stellen (art. 3, lid 8, sub c), om uitvoeringshandelingen vast te stellen over de gevallen waarin Data Protection Impact Assessments (DPIA's) verplicht zijn (art. 3, lid 9, sub b) en om uitvoeringshandelingen vast te stellen om criteria en middelen te omschrijven om zo te bepalen wanneer er geen sprake meer is van persoonsgegevens bij pseudonimisering (art. 3, lid 10). In het BNC-fiche lezen deze leden dat de regering *"hier een risico ziet van meer politieke besluitvorming, wat niet vanzelfsprekend past bij een verordening die mede strekt tot grondrechtenbescherming"*.⁶ Deze leden zien dit risico ook en vinden dit een zeer onwenselijke ontwikkeling.

Deze leden lezen voorts in het BNC-fiche dat het toekennen van de bevoegdheid van artikel 3, lid 10 van het voorstel aan de Europese Commissie "niet mogelijk" is volgens de regering. Omdat deze uitvoeringshandelingen die de Commissie op basis van dit artikel zou kunnen vaststellen betrekking hebben op de definitie van persoonsgegevens (artikel 41a), betreft dit een essentieel onderdeel van de basishandeling, dat zich "niet leent" voor uitwerking in uitvoeringshandelingen, aldus de regering. Dergelijke uitvoeringshandelingen zouden bovendien mogelijk betrekking hebben op de reikwijdte van het grondrecht op bescherming van persoonsgegevens. De AVG is immers een uitwerking van het recht op gegevensbescherming.

Daarnaast krijgt de Europese Commissie in artikel 1, lid 25, sub c, van het voorstel de bevoegdheid om uitvoeringshandelingen vast te stellen waarin handhavingsbevoegdheden van de Europese Commissie worden bepaald, waaronder het opleggen van boetes en andere sancties (wijziging van artikel 75 van de AI-verordening). Ook het toekennen van deze bevoegdheid om handhavingsbevoegdheden vast te stellen is "niet mogelijk" volgens de regering. De regering acht het toekennen van handhavingsbevoegdheden aan de Europese Commissie, waarbij een evenwicht moet worden gevonden tussen de uiteenlopende belangen die aan de orde zijn, "niet acceptabel".

20. Er worden in het BNC-fiche verschillende termen gebruikt om de wijziging van de bevoegdheden van de Europese Commissie te duiden, waaronder "niet leent", "niet acceptabel" en "niet mogelijk". Kunt u een preciezer juridisch oordeel geven over alle voorgestelde wijzigingen van de bevoegdheden? Deze leden ontvangen daarbij graag per wijziging van bevoegdheid een afzonderlijk oordeel, evenals een nadere juridische duiding van het mogelijk effect op de reikwijdte van het recht op bescherming van persoonsgegevens.

21. Wat is uw strategie om dit onderdeel van de Omnibus Digitaal aangepast te krijgen?

⁶ Kamerstukken I 2025/26, 36.890, A, p. 7.



datum 24 februari 2026

ons kenmerk 179856

blad 5

22. Hoe ligt het Europese krachtenveld ten aanzien van deze aanpassingen?
23. Is aanpassing van dit onderdeel een harde randvoorwaarde om in te kunnen stemmen met de Omnibus Digitaal?

e. Nationale veiligheid

De leden van de fractie van GroenLinks-PvdA merken op dat door de inrichting van een Europees meldpunt een deel van de nationale dienstverlening rondom incidentenafhandeling verschuift naar Europees niveau. Dit geldt ook voor meldingen onder de NIS2 en CER, waar incidenten bij de Rijksoverheid en vitale infrastructuur gevoelige informatie omtrent nationale veiligheid kunnen bevatten.

In het BNC-fiche wordt benadrukt dat *"nationale meldstructuren, waarbij lidstaten de directe en primaire ontvanger van incidentinformatie blijven, behouden moeten blijven"*.⁷ Ook staat in het BNC-fiche dat de regering daarnaast zorgen heeft *"omtrent beveiligingsrisico's als het gaat om het centraliseren van dergelijke meldplichten binnen één meldpunt. Het verwerken van zeer gevoelige meldingen, en in het bijzonder incidentinformatie van 27 lidstaten is namelijk erg kwetsbaar en een zaak van nationale veiligheid. Daarbij ziet het kabinet ook risico's ten aanzien van de afhankelijkheid van de continuïteit van een platform dat op EU-niveau wordt beheerd"*.⁸

24. Kunt u nader toelichten welke kwetsbaarheden in het kader van de (nationale) veiligheid voorzien worden?
25. Wat is uw strategie om dit onderdeel van de Omnibus Digitaal aangepast te krijgen?
26. Hoe ligt het Europese krachtenveld rondom deze aanpassingen?
27. Is aanpassing van dit onderdeel een harde randvoorwaarde om in te kunnen stemmen met de Omnibus Digitaal?

In het kader van de proportionaliteitsbeoordeling lezen deze leden in het BNC-fiche dat de regering vraagtekens heeft over de proportionaliteit van de voorstellen ten aanzien van een Europees meldpunt: *"De tweede kanttekening is dat het kabinet zorgen heeft ten aanzien van de inrichting van een Europees meldpunt. Volgens het kabinet is door de Commissie onvoldoende inzichtelijk gemaakt of een Europees meldpunt daadwerkelijk zal zorgen voor lastenverlichting en simplificatie, in het bijzonder waar het gaat om niet-grensoverschrijdende entiteiten. Ook is onvoldoende duidelijk wat de omvang is van de groep entiteiten die wel voordeel zouden kunnen hebben bij een Europees meldpunt, namelijk de grensoverschrijdende entiteiten en/of (grensoverschrijdende) entiteiten die rapportageverplichtingen hebben die onder meerdere wetgevingskaders vallen, bijvoorbeeld AVG én NIS2-richtlijn. Om die reden heeft het kabinet twijfels over de geschiktheid van deze maatregel in het licht van het doel om regeldruk te verlagen"*.⁹

28. Is er inmiddels meer helderheid over de geconstateerde onduidelijkheden?
29. Heeft u een nader oordeel over de proportionaliteit van dit onderdeel?

f. Uitstellen verplichtingen met betrekking tot hoog risico AI-systemen

⁷ Kamerstukken I 2025/26, 36.890, A, p. 8.

⁸ Kamerstukken I 2025/26, 36.890, A, p. 8.

⁹ Kamerstukken I 2025/26, 36.890, A, p. 12-13.



datum 24 februari 2026

ons kenmerk 179856

blad 6

De EDPB en de EDPS hebben in een gezamenlijke opinie over de Omnibus AI gepleit om de verplichtingen volgens de oorspronkelijke planning in te laten gaan.¹⁰ De leden van de fractie van GroenLinks-PvdA maken zich, gezien de razendsnelle ontwikkelingen van AI-systemen, zorgen over het uitstellen van de verplichtingen met betrekking tot hoog risico AI-systemen. Met deze voorstellen worden verplichtingen met respectievelijk zestien maanden en twaalf maanden vertraagd, waarbij de inwerkingtreding wordt gekoppeld aan een Commissiebesluit.

30. Hoe oordeelt u over dit advies van de EDPB en de EDPS? Deze leden ontvangen graag een toelichting.
31. Deelt u de zorgen van deze leden? Zo nee, waarom niet?
32. Kunt u een inschatting maken van de mogelijke effecten, waaronder op ondernemers die door deze aanpassing geen vaste invoeringsdatum kennen?
33. Hoe ligt het Europese krachtenveld ten aanzien van deze aanpassingen?
34. Is aanpassing van dit onderdeel een harde randvoorwaarde om in te kunnen stemmen met de Omnibus AI?

De laatste maanden is er veel te doen over digitale autonomie en minder afhankelijkheid van de grote (Amerikaanse) techbedrijven.

35. Past deze aanpassing in de actuele strategie om minder afhankelijk te worden van de grote (Amerikaanse) techbedrijven? Deze leden ontvangen graag een toelichting.

Deze leden horen veel zorgen over de zogenaamde AI-gedreven 'nudifier' tools.

36. Deelt u deze zorgen? Zo nee, waarom niet?
37. Is de regering bereid om in Europa te pleiten voor een verbod op deze tools, bijvoorbeeld in artikel 5 van de AI-verordening?

g. Schrappen registratieplicht hoog risico AI-systemen

De EDPB en de EDPS hebben in een gezamenlijke opinie over de Omnibus AI gepleit om de voorgenomen aanpassingen van de registratieplicht van hoog risico AI-systemen niet door te voeren omdat dit transparantie en toezicht ondermijnt en misbruik in de hand kan werken.¹¹

In het BNC-fiche lezen deze leden dat de regering bezwaren heeft *"tegen het schrappen van de registratieplicht voor hoog-risico AI die alleen voor beperkte of procedurele taken worden gebruikt. Dit de transparantie verlaagt over het gebruik van AI-systemen in hoog risico context en bemoeilijkt het toezicht op deze systemen. Bovendien levert deze maatregel slechts een beperkte verlichting van regeldruk op"*.¹²

39. Hoe oordeelt u over het advies van de EDPB en de EDPS? Deze leden ontvangen graag een toelichting.
40. Wat is uw proportionaliteitsoordeel op dit onderdeel?

¹⁰ EDPB-EDPS Joint Opinion 1/2026 On the Proposal for a regulation as regards the simplification on the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI), p. 14-15.

¹¹ EDPB-EDPS Joint Opinion 1/2026 On the Proposal for a regulation as regards the simplification on the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI), p. 8-9.

¹² Kamerstukken I 2025/26, 36.890, A, p. 9.



datum 24 februari 2026

ons kenmerk 179856

blad 7

41. Kunt u een nadere toelichting geven op de wijze waarop het toezicht bemoeilijkt wordt en wat de gevolgen daarvan kunnen zijn?
42. Wat is uw strategie om dit onderdeel van de Digitale Omnibussen aangepast te krijgen?
43. Hoe ligt het Europese krachtenveld ten aanzien van deze aanpassingen?
44. Is aanpassing van dit onderdeel een harde randvoorwaarde voor u om in te kunnen stemmen met de Omnibus AI?

De laatste maanden is er veel te doen over digitale autonomie en minder afhankelijkheid van de grote (Amerikaanse) techbedrijven.

45. Past deze aanpassing in de actuele strategie om minder afhankelijk te worden van de grote (Amerikaanse) techbedrijven? Deze leden ontvangen graag een toelichting.

h. Rol van Europese en nationale toezichthouders

De leden van de fractie van GroenLinks-PvdA merken op dat het belangrijk is om een goed niveau van toezicht te borgen. De EDPB en EDPS uiten zorgen over de positie van de nationale toezichthouders (o.a. verlies bevoegdheden en onafhankelijkheid) en de taakafbakening van en de samenwerking met het AI-bureau.¹³ Ook zijn er grote zorgen over het gebrek aan capaciteit bij zowel de nationale toezichthouders als het AI-bureau om duizenden bedrijven te controleren op wat er "onder de motorkap" van een AI-systeem gebeurt.

46. Hoe oordeelt u over de zorgen van de EDPB en EDPS? Deze leden ontvangen graag een toelichting.
47. Wat is volgens u nodig aan capaciteit (nationaal en Europees) om de toezichthoudende taak goed uit te voeren? Deze leden ontvangen graag een toelichting.
48. Is goed toezicht een harde randvoorwaarde om in te kunnen stemmen met de Omnibus Digitaal en de Omnibus AI?

In het BNC-fiche lezen deze leden dat de regering de gevolgen voor de handhaafbaarheid onderzoekt, maar niet verwacht dat de voorstellen tot significante nieuwe uitdagingen met betrekking tot de uitvoering van de onderliggende Europese wetten leidt omdat de voorstellen beogen de wetgeving te versimpelen.

In het BNC-fiche lezen deze leden verder: *"Het voorstel zal implicaties hebben voor het toezicht op verschillende Europese regelgeving, dat nationaal is ingericht. Naar verwachting kunnen die taken worden ondergebracht bij de toezichthouders die nu al op deze Europese regelgeving toezien. Daarbij wordt gezocht naar de meest doeltreffende en doelmatige oplossing. Of de aanpassingen de kosten voor het toezicht en de handhaving zullen verhogen of verlagen is nog niet duidelijk. Het voorstel bevat ook enkele bepalingen die de AVG wijzigen en er mogelijk voor zullen zorgen dat er meer meldingen ontstaan bij de toezichthoudende autoriteit en de rechtspraak. Het kabinet verwacht niet dat er een omvangrijke verhoging in kosten van toezicht en handhaving zal zijn. Het versimpelen van de regels kan ook handhaving en toezicht vergemakkelijken. Het kabinet zal dit verder onderzoeken en opheldering vragen bij de Europese Commissie. De budgettaire gevolgen voor de Rijksbegroting worden ingepast op de begroting van de beleidsverantwoordelijke*

¹³ EDPB-EDPS Joint Opinion 1/2026 On the Proposal for a regulation as regards the simplification on the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI), p. 11-12.



datum 24 februari 2026

ons kenmerk 179856

blad 8

departementen, volgens de regels van de budgetdiscipline. Daarbij dient ook rekening gehouden te worden met medeoverheden".¹⁴

49. Is dit nader onderzoek reeds afgerond? Zo ja, wat is daarvan de uitkomst?
50. Hoe verhoudt de passage in het BNC-fiche zich tot de zorgen over de handhaafbaarheid vanuit de toezichthouders? Deze leden ontvangen graag een toelichting.

i. Definitie persoonsgegevens en trainen AI-modellen

In het BNC-fiche lezen deze leden dat de regering ziet dat sommige aanpassingen aan de AVG een fundamentele impact hebben op het recht op privacy en het recht op gegevensbescherming, maar dat bij gebrek aan *impact assessment* en advies van de EPDB en EDPS de regering de proportionaliteit ervan niet kan beoordelen. Inmiddels zijn, na het verschijnen van de BNC-fiches, de adviezen van de EDPS en het EDPB verschenen.¹⁵

51. Hoe beoordeelt u deze adviezen?
52. Kunt u nogmaals reflecteren op de proportionaliteit van de aanpassingen aan de AVG na het lezen van de adviezen van de EPDB en EDPS?
53. Wat betekent dit voor het oordeel van de regering ten aanzien van de proportionaliteit van de Omnibus Digitaal en de Omnibus AI? Deze leden ontvangen graag een toelichting.

Het wijzigen van de definitie van persoonsgegevens in de Omnibus Digitaal heeft als voornaamste effect dat het trainen van AI-modellen makkelijker en juridisch toegankelijker wordt. De voorgestelde wijzigingen verkleinen de reikwijdte van wat als 'persoonsgegevens' wordt beschouwd, waardoor meer data gebruikt kan worden zonder expliciete toestemming van de betrokkenen. Het voorstel kent een aantal wijzigingen ten aanzien van de definitie en reikwijdte van persoonsgegevens, namelijk:

Nauwere definitie van persoonsgegevens: informatie die niet direct kan leiden tot identificatie van een persoon (bijvoorbeeld bepaalde gepseudonimiseerde data) wordt niet meer als 'persoonsgegeven' gezien als de ontvanger niet over de middelen beschikt om de persoon te identificeren. Dit maakt het eenvoudiger om grote datasets te gebruiken voor AI-training.

54. Wie is verantwoordelijk voor de beoordeling of de ontvanger niet over voldoende middelen beschikt om de persoon te identificeren; de afzender of de ontvanger? Wat betekent dit praktisch in de hele keten van informatie-uitwisseling?
55. Er is ook veel data die niet direct, maar indirect gegevens onthult. Bijvoorbeeld politieke voorkeur die afgeleid kan worden uit reacties en *likes* op een platform. Ook indirecte gegevens zoals locatiegegevens, surfgedrag, of aankoopgeschiedenis kunnen makkelijker worden gebruikt. Wat betekent deze aanpassing voor het beschermingsniveau? Deze leden ontvangen graag een toelichting.
56. De Autoriteit Persoonsgegevens (AP) waarschuwt voor het risico op grootschalige surveillance als indirecte identificatie niet meer onder de AVG valt. Het wordt makkelijker

¹⁴ Kamerstukken I 2025/26, 36.890, A, p. 13.

¹⁵ EDPB-EDPS Joint Opinion 1/2026 On the Proposal for a regulation as regards the simplification on the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI). EDPB-EDPS Joint Opinion 2/2026 On the Proposal for a Regulation as regards the simplification of the digital legislative framework (Digital Omnibus).



datum 24 februari 2026

ons kenmerk 179856

blad 9

om op basis van "anonieme" data profielen te maken die in de praktijk alsnog naar individuen herleidbaar zijn, wat kan leiden tot ongewenste monitoring. Hoe oordeelt u over dit risico? Deze leden ontvangen graag een toelichting.

57. De EDPB en EDPS waarschuwen dat de 'versmalling' van de definitie van persoonsgegevens een juridisch gat creëert: als data niet langer als 'persoonlijk' wordt gezien, vervallen alle AVG-waARBorgen automatisch, waardoor de nieuwe 'extra' regels weinig effect hebben.¹⁶ Hoe oordeelt u over dit risico?
58. Hoe oordeelt u over deze aanpassing als geheel?
59. Wat betekent deze aanpassing voor het toezicht? Welke (mogelijke) knelpunten worden hierbij voorzien?
60. Wat betekent deze aanpassing voor de (grond)rechten/positie van burgers/consumenten? Deze leden ontvangen graag een toelichting.

De laatste maanden is er veel te doen over digitale autonomie en minder afhankelijkheid van de grote (Amerikaanse) techbedrijven.

61. Past deze aanpassing in de actuele strategie om minder afhankelijk te worden van de grote (Amerikaanse) techbedrijven? Deze leden ontvangen graag een toelichting.

Ruimere interpretatie van 'legitiem belang': het trainen van AI-modellen en het doen van wetenschappelijk onderzoek worden expliciet erkend als legitieme belangen onder de AVG. Hierdoor is geen toestemming nodig, mits er passende waarborgen zijn. De Omnibus Digitaal erkent expliciet dat onderzoek door commerciële partijen, zoals het trainen van AI-modellen door een techbedrijf, als wetenschappelijk onderzoek kan worden aangemerkt, mits het bijdraagt aan de algemene stand van de techniek en wetenschap.

62. Hoe oordeelt u over de voorgestelde waarborgen?
63. Hoe oordeelt u over deze aanpassing als geheel?
64. Wat betekent deze aanpassing voor het toezicht? Welke (mogelijke) knelpunten worden hierbij voorzien?
65. Wat betekent deze aanpassing voor de (grond)rechten/positie van burgers/consumenten? Deze leden ontvangen graag een toelichting.

Onder andere de European Digital Rights (EDRi), een koepelorganisatie van burgerrechtenorganisaties, waarschuwt dat de Omnibus Digitaal een "vrijbrief" geeft aan grote (Amerikaanse) techbedrijven om de AVG te omzeilen door middel van een vage definitie over "wetenschappelijk onderzoek" en "gerechtvaardigd belang" bij het trainen van AI.¹⁷

66. Kunt u reflecteren op deze waarschuwing? Deze leden ontvangen graag een toelichting.
67. Deelt u de opvatting dat het legitimeren van dataverzameling voor het trainen van AI-systemen zonder toestemming uitsluitend de machtspositie van grote spelers zal versterken, die reeds over gigantisch veel data beschikken, en dat dit schadelijk is voor privacy van EU-burgers en eerlijke concurrentie met Europese bedrijven?

¹⁶ EDPB-EDPS Joint Opinion 2/2026 On the Proposal for a Regulation as regards the simplification of the digital legislative framework (Digital Omnibus), p. 9-12.

¹⁷ EDRi, 'Why the Digital Omnibus puts GDPR and ePrivacy at risk', [202511-Eexplaining-GDPR_eprivacy-Digital-Omnibus.pdf](#).



datum 24 februari 2026

ons kenmerk 179856

blad 10

De laatste maanden is er veel te doen over digitale autonomie en minder afhankelijkheid van de grote (Amerikaanse) techbedrijven.

68. Past deze aanpassing in de actuele strategie om minder afhankelijk te worden van de grote (Amerikaanse) techbedrijven? Deze leden ontvangen graag een toelichting.

Gebruik van gevoelige data voor bias-detectie: het gebruik van bijzondere persoonsgegevens over bijvoorbeeld etniciteit, religie of gezondheid, voor het opsporen en corrigeren van bias in AI-systemen wordt verruimd. Zo wordt de doelgroep voor het gebruik van data voor bias-detectie verruimd: waar de AI-verordening deze uitzondering momenteel beperkt tot aanbieders van hoog-risico systemen, breidt de Omnibus AI dit uit naar aanbieders én gebruikers van alle AI-systemen en -modellen.

69. Hoe oordeelt u over deze aanpassing?

70. Wat betekent deze aanpassing voor het toezicht? Welke (mogelijke) knelpunten worden hierbij voorzien?

71. Wat betekent deze aanpassing voor de (grond)rechten/positie van burgers/consumenten? Deze leden ontvangen graag een toelichting.

Organisaties mogen biometrische gegevens verwerken wanneer het noodzakelijk is om de identiteit van een betrokkene te verifiëren en de gegevens en middelen voor deze verificatie onder de uitsluitende controle van de betrokkene zijn.

72. Wat betekent precies "onder uitsluitende controle van betrokkenen zijn" in de situatie waarbij een werkgever dit wil gebruiken voor de toegangscontrole van medewerkers?

De EDPB en EDPS uiten kritiek op het feit dat de Omnibus AI voorziet in een wijziging van de grondslag voor de verwerking van bijzondere persoonsgegevens, waarbij de eis van "strikt noodzakelijk" wordt vervangen door de minder strenge eis van "noodzakelijk".¹⁸

73. Hoe oordeelt u over deze specifieke aanpassing?

74. Wat betekent deze aanpassing voor het toezicht? Welke (mogelijke) knelpunten worden hierbij voorzien?

75. Wat betekent deze aanpassing voor de (grond)rechten/positie van burgers/consumenten? Deze leden ontvangen graag een toelichting.

De Europese Commissie stelt enkele waarborgen voor, namelijk:

- Strikte doelbinding: De verwerking van gegevens over gezondheid, religie of etniciteit is alleen toegestaan voor het detecteren en corrigeren van bias. Zodra de bias is verholpen, moet de data in principe worden verwijderd of geanonimiseerd.
- Beperkte toegang: Alleen geautoriseerd personeel mag met deze gevoelige datasets werken. Er moeten technische barrières zijn (zoals 'clean rooms' of beveiligde omgevingen) om te voorkomen dat de data weglekt naar andere afdelingen.

¹⁸ EDPB-EDPS Joint Opinion 1/2026 On the Proposal for a regulation as regards the simplification on the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI), p. 7.



datum 24 februari 2026

ons kenmerk 179856

blad 11

- Transparantie en documentatie: Ontwikkelaars moeten in hun technische documentatie vastleggen waarom het gebruik van deze data noodzakelijk was en welke maatregelen zijn genomen om de privacy te beschermen.
- Toezicht door het AI-bureau: Dit nieuwe Europese orgaan moet toezien op de naleving van deze regels bij de machtigste AI-modellen.
 - 76. Hoe oordeelt u over deze waarborgen?
 - 77. Wat betekent deze aanpassing voor het toezicht? Welke (mogelijke) knelpunten worden hierbij voorzien?
 - 78. Wat betekent deze aanpassing voor de (grond)rechten/positie van burgers/consumenten? Deze leden ontvangen graag een toelichting.

Nationale toezichthouders en de EDPB en EDPS waarschuwen voor:

- Het risico op '*function creep*'. Dit behelst het risico dat de data die verzameld worden voor bias-correctie in de praktijk voor andere (commerciële) doeleinden gebruikt kunnen worden zodra de drempel voor verwerking is verlaagd;
- Nieuwe vormen van profilering. Hoewel het doel "eerlijkheid" is, kunnen bedrijven deze gevoelige data indirect gebruiken om gedrag te voorspellen. Zo kan een verzekeraar of bank AI-modellen bouwen die patronen herkennen die samenhangen met religie of gezondheid, wat kan leiden tot uitsluiting op basis van statistische profielen.
- Inbreuk op de private sfeer. Gegevens over religie en etniciteit behoren tot de meest persoonlijke informatie. Critici vrezen dat het "normaliseren" van het gebruik hiervan in AI-training de psychologische drempel verlaagt voor overheden en bedrijven om deze data op grote schaal te monitoren.
 - 79. Hoe oordeelt u over deze voorziene risico's?
 - 80. Wat betekent dit voor het toezicht? Welke (mogelijke) knelpunten worden hierbij voorzien?
 - 81. Wat betekent dit de (grond)rechten/positie van burgers/consumenten? Deze leden ontvangen graag een toelichting.

De EDPB en EDPS vinden dat gebruik van gevoelige gegevens voor bias-detectie alleen zou mogen in strikt afgebakende situaties, bijvoorbeeld wanneer de risico's van discriminatie ernstig zijn en er passende waarborgen gelden.¹⁹ De EDPB en EDPS adviseren om het gebruik van gevoelige gegevens (zoals etniciteit of gezondheidsdata) voor bias-detectie expliciet te beperken tot gevallen waarin het risico op ernstige nadelige gevolgen door bias aangetoond kan worden.

82. Kunt u reflecteren op dit advies? Onderschrijft u deze voorwaarde?

83. Is aanpassing van dit onderdeel een harde randvoorwaarde om in te kunnen stemmen met de Omnibus AI?

De EDPB en EDPS benadrukken dat nationale gegevensbeschermingsautoriteiten in de eerste plaats bevoegd zouden moeten zijn om toezicht te houden op de verwerking van persoonsgegevens.²⁰

84. Hoe oordeelt u over dit advies? Onderschrijft u deze voorwaarde?

¹⁹ EDPB-EDPS Joint Opinion 1/2026 On the Proposal for a regulation as regards the simplification on the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI), p. 6-8.

²⁰ EDPB-EDPS Joint Opinion 1/2026 On the Proposal for a regulation as regards the simplification on the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI), p. 8.



datum 24 februari 2026

ons kenmerk 179856

blad 12

85. Is aanpassing van dit onderdeel een harde randvoorwaarde om in te kunnen stemmen met de Omnibus AI?

In het kader van de proportionaliteitsbeoordeling lezen de leden van de fractie GroenLinks-PvdA in het BNC-fiche dat de regering vraagtekens heeft over de proportionaliteit van de voorstellen ten aanzien van de gegevensbescherming in relatie tot de vermindering van de regeldruk: *"Sommige wijzigingen aan de AVG lijken verder te gaan dan noodzakelijk omdat de wijzigingen afbreuk doen aan respectievelijk gegevensbescherming en onvoldoende duidelijk is in hoeverre deze voorstellen effectief regeldruk verlagen. Het kabinet zal opheldering vragen bij de Commissie en de gevolgen voor regeldruk, uitvoerbaarheid en bescherming van grondrechten verder in kaart te brengen voordat het tot een definitief oordeel komt op deze onderdelen. Het kabinet hecht eraan dat er in het bijzonder voor wijzigingen met impact op gegevensbescherming en fundamentele rechten gelegenheid is om de voorstellen en de gevolgen daarvan gedegen te analyseren en deze inhoudelijk te bespreken".*²¹

86. Is er inmiddels meer helderheid over de geconstateerde onduidelijkheden?

87. Is een nader oordeel over de proportionaliteit van dit onderdeel?

De laatste maanden is er veel te doen over digitale autonomie en minder afhankelijkheid van de grote (Amerikaanse) techbedrijven.

88. Past deze aanpassing in de actuele strategie om minder afhankelijk te worden van de grote (Amerikaanse) techbedrijven? Deze leden ontvangen graag een toelichting.

j. Geautomatiseerde besluitvorming

De leden van de fractie van GroenLinks-PvdA merken op dat artikel 22 van de AVG fundamenteel wordt herzien. Op dit moment heeft een betrokkene het recht om niet onderworpen te worden aan geautomatiseerde besluitvorming zonder menselijke tussenkomst als dat een rechtsgevolg of ander gevolg heeft dat hem of haar significant raakt. Daar zijn een aantal uitzonderingen op. Deze negatieve formulering 'mag niet, behalve' wordt in het voorstel omgedraaid naar een positieve formulering: het mag als er aan bepaalde voorwaarden wordt voldaan.

89. Hoe oordeelt u over deze aanpassing?

90. Wat betekent dit voor het toezicht? Welke mogelijke knelpunten worden hierbij voorzien?

91. Wat betekent dit de (grond)rechten/positie van burgers/consumenten? Deze leden ontvangen graag een toelichting.

De laatste maanden is er veel te doen over digitale autonomie en minder afhankelijkheid van de grote (Amerikaanse) techbedrijven.

92. Past deze aanpassing in de actuele strategie om minder afhankelijk te worden van de grote (Amerikaanse) techbedrijven? Deze leden ontvangen graag een toelichting.

k. Effecten gecentraliseerde toestemming voor het Nederlandse en Europese medialandschap

De leden van de fractie van GroenLinks-PvdA lezen in een position paper van NDP Nieuwsmedia, een branchevereniging voor nieuwsmedia, dat zij bezorgd zijn over de aangekondigde Omnibus

²¹ Kamerstukken I 2025/26, 36.890, A, p. 12.



datum 24 februari 2026

ons kenmerk 179856

blad 13

Digitaal.²² De Omnibus Digitaal grijpt volgens NDP Nieuwsmedia op onwenselijke wijze in op Nederlandse nieuwsmedia en brengt daarmee het behoud van een vitaal Nederlands journalistiek landschap in gevaar, omdat steeds meer advertentie-inkomsten richting Big-Tech vloeien. Juist in een tijd waarin grote (Amerikaanse) techbedrijven steeds meer invloed krijgen op de informatievoorziening, is het behoud van een vitaal journalistiek landschap van groot maatschappelijk belang.

Deze leden lezen dat de Europese Commissie de kwetsbare positie van nieuwsuitgevers op de online advertentiemarkt erkent. Dit is onder meer aanleiding geweest voor het *European Democracy Shield*, waarmee wordt ingezet op duurzame bescherming van Europese nieuwsuitgevers.

93. Herkent u, net als de Europese Commissie, het belang om de positie van nieuwsuitgevers binnen Omnibus Digitaal extra te beschermen ten opzichte van grote (Amerikaanse) techbedrijven? Deze leden ontvangen graag een toelichting.

De Europese Commissie poogt nieuwsuitgevers binnen de Omnibus Digitaal te beschermen door hen uit te zonderen van gecentraliseerde cookie-toestemming voor de verwerking van persoonsgegevens (art. 88ter, lid 3). Deze uitzondering voor mediadiensten is noodzakelijk om te voorkomen dat het financieren van journalistiek middels advertenties nagenoeg onmogelijk wordt, maar de invoering van 'één klik' (art. 88bis, lid 4, sub a) leidt er alsnog toe dat de financiering van de journalistiek volgens NPD Nieuwsmedia ernstig in gevaar wordt gebracht. De gecentraliseerde cookie-toestemming vergroot de marktmacht van grote (Amerikaanse) techbedrijven. Hoewel zij op grote schaal data verzamelen en persoonsgericht adverteren, zullen zij minder geraakt worden door dit voorstel, omdat ze in mindere mate gebruik van cookie-toestemming bij hun dataverzameling en targeting.

94. Herkent u het risico dat de voorgestelde maatregelen binnen de Omnibus Digitaal de marktmacht van grote (Amerikaanse) techbedrijven op de online advertentiemarkt juist verder vergroot, terwijl grote (Amerikaanse) techbedrijven door steeds groter wordende marktmacht de duurzame financiering van de Nederlandse journalistiek bedreigt? Deze leden ontvangen graag een toelichting.

Tot slot hebben de leden van de fractie van GroenLinks-PvdA van NDP Nieuwsmedia vernomen dat zij verwachten dat de uitzondering in de praktijk ertoe zal leiden dat grote Amerikaanse techbedrijven (zoals Google) bepalen wat kan worden gekwalificeerd als *media service provider* in de zin van de Media Freedom Act. Dit vergroot de marktmacht van de digitale gatekeepers, zoals bedoeld in de Digital Markets Act (DMA).

95. Erkent u dit risico? Zo nee, waarom niet? Zo ja, acht u het wenselijk om hier iets aan te doen? Deze leden ontvangen graag een toelichting.

I. Bezwaarmogelijkheden burgers

Met de wijzigingen van de AVG waarin de Omnibus Digitaal voorziet wordt het recht om bezwaar te maken tegen de verwerking van persoonsgegevens van artikel 21 van de AVG beperkt, nu de

²² NDP Nieuwsmedia, 'Digital Omnibus moet journalistiek beter beschermen, 4 februari 2026, <https://www.ndpnieuwsmedia.nl/2026/02/04/ndp-nieuwsmedia-digital-omnibus-moet-journalistiek-beter-beschermen/>.



datum 24 februari 2026

ons kenmerk 179856

blad 14

bewijslast en de drempels verschuiven. Het trainen van AI wordt bijvoorbeeld vaker aangemerkt als een gerechtvaardigd belang. Burgers moeten in dat geval aantonen dat hun concrete privacybelang zwaarder weegt dan het innovatiebelang van het bedrijf. Dat vormt een aanzienlijk hogere drempel dan tot nu toe het geval was.

96. Hoe oordeelt u over de wijzingen ten aanzien van de bezwaarmogelijkheden van burgers en maatschappelijke organisaties?

De EDPB en EDPS waarschuwen dat burgers niet meer kunnen overzien waar hun gegevens terechtkomen als het trainen van AI automatisch als 'gerechtvaardigd belang' wordt aangemerkt.²³

97. Hoe oordeelt u over deze zorgelijke conclusie van de EDPB en EDPS? Deze leden ontvangen graag een toelichting.

98. Hoe beoordeelt u de kritiek op dit onderwerp van onafhankelijke organisaties en consumentenbonden, zoals BEUC en Corporate Europe Observatory?²⁴

m. Gevolgen voor (mede)overheden en de rechtspraak

De leden van de fractie van GroenLinks-PvdA lezen dat de Omnibus Digitaal voorziet in een beperking van de reikwijdte van de bevoegdheid van overheden om gegevens op te vragen bij bedrijven in situaties van 'uitzonderlijke noodzaak' tot alleen 'algemene noodsituaties'. Dit is volgens de regering een verbetering voor het recht op gegevensbescherming.

99. Kunt u aangeven wat deze aanpassing betekent voor (mede)overheden? In welke situaties van 'uitzonderlijke noodzaak' kunnen (mede)overheden nu geen informatie meer opvragen? Deze leden ontvangen graag een toelichting met een aantal voorbeelden.

100. Kunt u aangeven hoe vaak dit soort situaties van 'uitzonderlijke noodzaak' in de afgelopen jaren zijn voorgekomen?

101. Kunt u een inschatting geven van de effecten van deze aanpassing?

De laatste maanden is er veel te doen over digitale autonomie en minder afhankelijkheid van de grote (Amerikaanse) techbedrijven.

102. Past deze aanpassing in de actuele strategie om minder afhankelijk te worden van de grote (Amerikaanse) techbedrijven? Deze leden ontvangen graag een toelichting.

In het BNC-fiche lezen deze leden dat er ook mogelijke effecten zijn voor de rechtspraak.

103. Welke effecten, en in welke omvang, worden door u voorzien? Wat is het oordeel van de partijen in de rechtspraak wat betreft de effecten van deze aanpassingen?

De leden van de fractie van GroenLinks-PvdA hebben van IPO en de VNG vernomen dat zij zich zorgen maken over risico's op surveillance bij bias-detectie, de gelijkschakeling van commerciële AI-

²³ EDPB-EDPS Joint Opinion 1/2026 On the Proposal for a regulation as regards the simplification on the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI), p. 16-17.

²⁴ The European Consumer Organisation (BEUC), 'EU's plan to simplify digital laws to benefit mainly large companies at the expense of consumers', 19 november 2025, <https://www.beuc.eu/press-release/eus-plan-simplify-digital-laws-benefit-mainly-large-companies-expense-consumers>; en Corporate Europe Observatory, 'Article by article, how Big Tech shaped the EU's roll-back of digital rights', 14 januari 2026, <https://corporateeurope.org/en/2026/01/article-article-how-big-tech-shaped-eus-roll-back-digital-rights>.



datum 24 februari 2026

ons kenmerk 179856

blad 15

training met wetenschappelijk onderzoek en de verschuiving van verantwoordelijkheid voor AI-geletterdheid. IPO en VNG wezen ook op mogelijke versnippering van toezicht, het schrappen van de registratieplicht voor AI-systemen, onduidelijkheid over gecentraliseerde incidentrapportage en de inperking van lokaal ethisch beleid.

104. Kunt u op alle genoemde punten inhoudelijk reageren? Hoe oordeelt u op deze kritiekpunten? Deze leden zien graag een reactie op de inperking van (decentraal) ethisch beleid.

n. Schrappen Platform-to-Business-verordening (P2B)

In het BNC-fiche lezen de leden van de fractie van GroenLinks-PvdA dat de regering kritisch is op het voorstel om de P2B-verordening gefaseerd in te trekken.

105. Wat is de strategie om dit onderdeel van de Digitale Omnibussen aangepast te krijgen?
106. Hoe ligt het Europese krachtenveld ten aanzien van deze aanpassingen?
107. Is aanpassing van dit onderdeel een harde randvoorwaarde om in te kunnen stemmen met de Omnibus Digitaal?

De ACM is sinds kort bevoegd om de P2B te handhaven en ontvangt, zo lezen deze leden in het BNC-fiche, inmiddels regelmatig meldingen over niet-naleving van de P2B door platforms: *"Zonder de P2B kan de ACM geen toezicht meer houden op problemen die ondernemers ondervinden op platforms die buiten Nederland gevestigd zijn"*.²⁵ Schrappen zal dus naar verwachting leiden tot minder rechtszekerheid en minder bescherming voor met name kleinere ondernemers die handelen op platforms.

108. Kunt u, in overleg met ACM, een nadere toelichting geven op welk type bedrijven zich niet aan de wetgeving houdt?
109. Kunt u, in overleg met ACM, toelichting geven op de verwachte impact van het schrappen van de P2B?

De laatste maanden is er veel te doen over digitale autonomie en minder afhankelijkheid van de grote (Amerikaanse) techbedrijven.

110. Past deze aanpassing in de actuele strategie om minder afhankelijk te worden van de grote (Amerikaanse) techbedrijven? Deze leden ontvangen graag een toelichting.

o. Uitzonderingsbepalingen overstappen clouddiensten

De leden van de fractie van GroenLinks-PvdA hebben grote zorgen over de uitzonderingen die in de Omnibus Digitaal worden geïntroduceerd met betrekking tot de bepalingen inzake het overstappen tussen clouddiensten. Overstappen is niet in alle gevallen meer gratis, maar er kunnen 'proportionele overstapvergoedingen' in rekening worden gebracht bij maatwerk-diensten. In het BNC-fiche lezen de leden dat deze uitzonderingen volgens de regering juist onduidelijkheid voor gebruikers van clouddiensten creëren en hun keuzevrijheid belemmeren. De regering ziet *"liever geen aanpassingen die de werking van dit onderdeel van de Dataverordening beperken of vertragen gezien de Dataverordening een belangrijk onderdeel is in het beter laten functioneren van de Europese cloudmarkt"*.²⁶

²⁵ Kamerstukken I 2025/26, 36.890, A, p. 10.

²⁶ Kamerstukken I 2025/26, 36.890, A, p. 10.



datum 24 februari 2026

ons kenmerk 179856

blad 16

111. Wat is de strategie om dit onderdeel van de Omnibus Digitaal aangepast te krijgen?
112. Hoe ligt het Europese krachtenveld ten aanzien van deze aanpassingen?
113. Is aanpassing van dit onderdeel een harde randvoorwaarde om in te kunnen stemmen met de Omnibus Digitaal?

De laatste maanden is er veel te doen over digitale autonomie en minder afhankelijkheid van de grote (Amerikaanse) techbedrijven.

114. Past deze aanpassing in de actuele strategie van Europa om minder afhankelijk te worden van de grote (Amerikaanse) techbedrijven? Deze leden ontvangen graag een toelichting.

p. AI-geletterdheid en registratieplicht hoog risico AI-systemen

De leden van de fractie van GroenLinks-PvdA merken op dat de verantwoordelijkheden omtrent AI-geletterdheid worden gewijzigd. De verplichtingen voor bedrijven om AI-geletterdheid te bevorderen worden verminderd. Deze verplichting geldt voortaan alleen voor organisaties die hoog risico AI-systemen inzetten. MBK-bedrijven worden grotendeels vrijgesteld van een actieve plicht om personeel te trainen. De verantwoordelijkheid om de algemene bevolking AI-geletterd te maken, wordt sterker bij de lidstaten zelf gelegd. Er wordt meer ruimte gegeven aan vrijwillige gedragscodes. In plaats van strikte wettelijke eisen voor training, mogen sectoren zelf bepalen wat een "voldoende niveau" van geletterdheid is voor hun specifieke werknemers.

In het BNC-fiche lezen deze leden dat de regering bezwaren heeft tegen het schrappen van de registratieplicht voor hoog risico AI die alleen voor beperkte of procedurele taken worden gebruikt omdat dit de transparantie verlaagt over het gebruik van AI-systemen in hoog risico context en het toezicht bemoeilijkt op deze systemen. Bovendien levert deze maatregel slechts een beperkte verlichting van regeldruk op, aldus de regering. De leden van de fractie van GroenLinks-PvdA maken zich zorgen over de effecten hiervan.

115. Wat is volgens u het effect hiervan? Deze leden ontvangen graag een toelichting.
116. Wat is het standpunt van u ten aanzien van deze wijzigingen? Deze leden ontvangen graag een toelichting.
117. Hoe denkt u deze verantwoordelijkheid binnen Nederland, samen met de medeoverheden, in te gaan vullen?

De EDPB en de EDPS hebben in een gezamenlijke opinie over de Omnibus AI bepleit dat bedrijven zelf verantwoordelijk dienen te blijven voor het waarborgen van voldoende kennis en zorgvuldigheid binnen hun organisatie.²⁷

118. Hoe oordeelt u over het advies van de EDPB en de EDPS? Deze leden ontvangen graag een toelichting.

q. Subsidiariteit

In het BNC-fiche lezen de leden van de fractie van GroenLinks-PvdA dat het de regering specifiek over het voorstel in de Omnibus Digitaal om een Europees meldpunt in te richten zorgen heeft over de subsidiariteit. De motivatie hiervoor is als volgt verwoord: "*Het specifieke doel van versimpelen*

²⁷ EDPB-EDPS Joint Opinion 1/2026 On the Proposal for a regulation as regards the simplification on the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI), p. 13-14.



datum 24 februari 2026

ons kenmerk 179856

blad 17

en stroomlijnen van de verschillende meldplichten uit (cyber)wetgeving kan voor een groot deel ook zonder dit vergaande middel bereikt worden en ook op nationaal niveau door lidstaten 12 worden opgelost. Zo zal de grootste groep entiteiten onder de CER- en de NIS2-richtlijn niet grensoverschrijdend opereren. Deze partijen hebben voldoende aan het simplificeren van rapportageverplichtingen en een meldpunt op nationaal niveau. Bovendien wordt er door lidstaten in diverse Europese expertgroepen, waaronder de NIS Cooperation Group, reeds samengewerkt om dit doel te bereiken".²⁸

119. Kunt u een nadere toelichting geven over de zorgen ten aanzien van de subsidiariteit? Is er volgens u wel of niet sprake van strijdigheid met het subsidiariteitsbeginsel op dit onderdeel?

r. Digital Fairness Act (DFA)

De leden van de fractie van GroenLinks-PvdA merken op dat de Digital Fairness Act (DFA) enerzijds, en de Omnibus Digitaal en de Omnibus AI anderzijds, deel uitmaken van een bredere beweging van de Europese Commissie om de digitale regelgeving te moderniseren, maar ze hebben tegenovergestelde doelen. Waar de DFA nieuwe regels toevoegt om consumenten te beschermen, zijn de Omnibus Digitaal en de Omnibus AI juist gericht op het verminderen van regeldruk (deregulering). De DFA voegt een nieuwe laag bescherming toe. Volgens de Europese Commissie is dit nodig omdat de huidige wetten (zoals de Unfair Commercial Practices Directive) "gaten" vertonen bij het aanpakken van moderne digitale problemen zoals *dark patterns* en verslavende algoritmes.

120. Hoe beoordeelt u deze tegenstelling? Deze leden ontvangen graag een toelichting.

121. Wordt met de Omnibus Digitaal en de Omnibus AI de doelstelling van de Digitale Fairness Act (DFA) aangetast? Zo ja, bij welke aanpassingen is dit volgens u aan de orde?

2. Vragen en opmerkingen van de leden van de fractie van de BBB

De leden van de fractie van de **BBB** hebben kennisgenomen van het BNC-fiche voor de Omnibus Digitaal en de Omnibus AI en het BNC-fiche voor de Data Unie Strategie. Deze leden merken op dat de invoering van de Omnibus Digitaal en de Omnibus AI leidt tot simplificatie en daardoor verhoging van de concurrentiekracht en verlaging van de administratieve lasten voor het bedrijfsleven. Zij wensen in dit kader enkele vragen te stellen aan u.

1. Wat is de totale geraamde besparing in administratieve lasten – uitgedrukt in euro's en fulltime-equivalenten (fte) – als gevolg van de Omnibus Digitaal en de Omnibus AI voor Nederlandse bedrijven in de komende vijf jaar?
2. Is er of wordt er een onafhankelijke *impact assessment* uitgevoerd op de Nederlandse situatie? Zo ja, kunt u deze impact assessment aan de Kamer doen toekomen?
3. Hoe waarborgt u dat de versoepelingen niet leiden tot een lagere bescherming van fundamentele rechten met betrekking tot privacy?
4. Op welke wijze wordt na invoering van de zevende omnibus ervoor gezorgd dat belanghebbenden op de hoogte zijn en worden getraind?
5. Is bij de berekening van besparingen rekening gehouden met deze kosten in tijd en geld?

²⁸ Kamerstukken I 2025/26, 36.890, A, p. 12.



datum 24 februari 2026

ons kenmerk 179856

blad 18

6. Welke knelpunten verwacht u bij het MKB en decentrale overheden (gemeenten en provincies) door de wijzigingen van de AI-verordening?
7. Hoe wordt ervoor gezorgd dat AI-leveranciers in Nederland de versoepelde eisen daadwerkelijk toepassen?
8. Acht u de voorgestelde inwerkingtredingstermijnen in de beide ontwerp-verordeningen – eenmaal vastgesteld en gepubliceerd – uitvoerbaar voor overheid en bedrijfsleven?
9. Worden er pilots voorzien om uitvoerbaarheid te testen?
10. In welke mate wordt het maatschappelijke middenveld zoals VNG, IPO, en MKB-Nederland betrokken?
11. Hoe voorkomt u dat versoepelingen leiden tot een *'race to the bottom'* bij AI-veiligheid?
12. Wat zijn de risico's op juridische procedures door onduidelijke overgangsregels?
13. Wordt de uitvoerbaarheid getoetst aan de hand van de Nederlandse Digitaliseringsstrategie (NDS)?
14. Hoe voorkomt u dat versoepelingen leiden tot meer meldingen bij de AP?
15. Voorziet u dat de Europese Commissie advies zal vragen aan de diverse adviesorganen?
16. Hoe blijft de AVG-compliance gewaarborgd na de voorgestelde wijzigingen?
17. Is er een aparte AVG-*impact assessment* uitgevoerd voor de Nederlandse situatie?

3. Vragen en opmerkingen van de leden van de fractie van D66, mede namens de leden van de fractie van de PvdD

De leden van de fractie van **D66** hebben met belangstelling kennisgenomen van het BNC-fiche voor de Omnibus Digitaal en de Omnibus AI en het BNC-fiche voor de Data Unie Strategie. Deze leden merken op dat het zeer brede en ingrijpende voorstellen zijn. Tegen deze achtergrond wensen deze leden, mede namens de leden van de fractie van de PvdD, nog een aantal vragen te stellen.

a. Vragen met betrekking tot COM(2025) 835 – Mededeling Data Unie Strategie

1. In het BNC-fiche geeft de regering met betrekking tot pijler I aan de nieuwe focus op *data spaces* te waarderen, maar merkt daarbij op dat belangrijke details in de uitwerking nog ontbreken. Ook geeft de regering aan in het voorstel een lange termijn visie te missen over *data spaces*. Wat is in uw ogen de lange termijn visie voor *data spaces*?
2. Verder wijst de regering erop, met betrekking tot pijler I, dat er nog uitdagingen liggen ten aanzien van het verantwoord delen van data. Deze leden vinden het belangrijk dat data verantwoord wordt gedeeld. Daarom vragen deze leden welke uitdagingen u ziet en hoe deze zich verhouden tot het waarborgen van fundamentele rechten.
3. Daarnaast heeft de regering, ten aanzien van dezelfde pijler, nog vragen of er overlap bestaat tussen bestaande activiteiten en de Data Labs. Deze leden vragen of u een beeld heeft van waar die mogelijke overlap plaatsvindt.
4. Gelet op de derde pijler merkt de regering op dat het de inzet op het versterken van partnerschappen met gelijkgestemde landen steunt, onder andere op het gebied van het inzetten van *data spaces* in internationale datastromen. Deze leden vragen wat u verstaat onder 'gelijkgestemde landen' en hoe u kijkt tegen het verder uitwerken (in EU-verband) van deze term, gelet op het belang dat onze data niet in verkeerde handen komt.



datum 24 februari 2026

ons kenmerk 179856

blad 19

b. Vragen met betrekking tot COM(2025) 836 en 837 –Omnibus AI en Omnibus Digitaal

5. De leden van de fractie van D66 onderschrijven dat de regering erop toeziet dat de Europese regelgeving doelgericht en uniform wordt geïmplementeerd, toegepast en gehandhaafd. De leden lezen in het BNC-fiche dat de regering het belang van voldoende capaciteit bij toezichthouders onderstreept. Deze leden vragen of u hiermee doelt op nationale of Europese toezichthouders en of naar uw oordeel de capaciteit momenteel toereikend is. Daarnaast merken de aan het woord zijnde leden op dat de Omnibus Digitaal voorziet in oprichting van een Europees meldpunt dat de rol van nationale toezichthouders lijkt over te nemen. Is er dan nog wel capaciteit bij onze nationale toezichthouder nodig?
6. Voorts geeft de regering in het BNC-fiche aan dat het belangrijk is dat er ruimte blijft voor nationale 'flexibiliteit' met betrekking tot het hergebruiken van persoonlijke data in publieke registers. Kunt u verduidelijken wat het in dit kader bedoelt met flexibiliteit?
7. Verder lezen de aan het woord zijnde leden in het BNC-fiche dat de Europese Commissie inschat dat de Omnibus AI €297 tot €433 miljoen aan lastenverlichting voor bedrijven oplevert en de Omnibus Digitaal zowel jaarlijks, als eenmalig, €1 miljard. Hoe beoordeelt u de verhouding tussen de mate van lastenverlichting die de Omnibussen opleveren en de beoogde doelen van vereenvoudiging en stroomlijning? Hoe beoordeelt u de omvang van de verwachte lastenverlichting? Mist u aspecten die in de Omnibussen hadden kunnen worden opgenomen die tot verdere besparingen hadden kunnen leiden en in lijn waren geweest met de gestelde doelen?
8. De regering plaatst twee kanttekeningen bij de proportionaliteit van de Europese voorstellen. Deze leden achten deze kanttekeningen vrij aanzienlijk en vragen waarom u desondanks positief oordeelt over de proportionaliteit van de Omnibus Digitaal en de Omnibus AI. Verwacht u dat deze aandachtspunten alsnog worden betrokken bij de verdere onderhandelingen?
9. Onlangs heeft de Autoriteit Persoonsgegevens (AP) in een position paper ook haar zorgen geuit over een aantal voorgestelde wijzigingen van de Omnibussen.²⁹ Zo gaat de drempel omhoog voor het melden van datalekken bij de toezichthouder op grond van de AVG. De Autoriteit Persoonsgegevens (AP) ziet in de praktijk dat organisaties de risico's van een datalek vaak bewust of onbewust onderschatten en geeft hier ook een concreet voorbeeld voor. Deze leden maken zich zorgen dat de autoriteit persoonsgegevens (AP) na de voorgestelde wijziging geen zicht meer heeft op deze gevallen. Deelt u deze zorg van deze leden?
10. Daarnaast geeft de Autoriteit Persoonsgegevens (AP) in het position paper aan dat de criteria voor de mogelijkheid om het recht op inzage in de AVG te beperken bij 'buitensporige verzoeken' niet duidelijk zijn. Hoe ziet u dit? Hoe beoordeelt u de zorg van de Autoriteit Persoonsgegevens (AP) dat deze onduidelijkheid ertoe zal leiden dat organisaties de term 'buitensporige verzoeken' verschillend zullen uitleggen?

4. Vragen en opmerkingen van de leden van de fractie van PVV

²⁹ Autoriteit Persoonsgegevens, 'Position paper AP: Omnibus Digitaal en Omnibus AI', 13 januari 2026, <https://www.autoriteitpersoonsgegevens.nl/documenten/position-paper-ap-omnibus-digitaal-en-omnibus-ai>.



datum 24 februari 2026

ons kenmerk 179856

blad 20

De leden van de fractie van **PVV** hebben kennisgenomen van het BNC-fiche voor de Omnibus Digitaal en de Omnibus AI en het BNC-fiche voor de Data Unie Strategie. Zij hebben nog een aantal vragen.

a. Vragen met betrekking tot COM(2025)836 – Omnibus AI

De leden van de PVV fractie merken op dat de Omnibus AI voorziet in: *"Het centraliseren van het toezicht door het AI-bureau op een groot aantal AI-systemen die zijn gebaseerd op AI-modellen voor algemene doeleinden of zijn ingebed in zeer grote onlineplatforms en zeer grote zoekmachines"*.³⁰

1. Kunt u aangeven óf en hoe op zo onafhankelijk mogelijke wijze en op gelijkwaardige basis AI-systemen beoordeeld zullen worden door het AI-bureau en op basis van welke concrete criteria?

In het voorstel van de Omnibus AI lezen de leden van de fractie van PVV dat wordt gewerkt aan aanvullende richtsnoeren die gericht zijn op het verstrekken van duidelijke en praktische instructies om de AI-verordening aan andere EU-wetgeving toe te passen. Daarbij gaat het onder meer om: *"richtsnoeren inzake het melden van ernstige incidenten door aanbieders van AI systemen met een hoog risico; richtsnoeren inzake de praktische toepassing van de vereisten met betrekking tot systemen met een hoog risico; richtsnoeren inzake de praktische toepassing van de verplichtingen voor aanbieders en gebruiksverantwoordelijken van AI-systemen met een hoog risico; richtsnoeren met een model voor de effectbeoordeling van de grondrechten."*³¹

2. Kunt u aangeven wat wordt verstaan onder 'ernstige incidenten', wat daarvoor de omschrijving is, wat de criteria zijn en door wie bepaald wordt wanneer sprake is van een 'ernstig incident'?
3. Kunt u aangeven wat wordt verstaan onder 'een hoog risico', wat daarvoor de omschrijving is, wat de criteria zijn en door wie bepaald wordt wanneer sprake is van een 'hoog risico'?
4. Kunt u aangeven hoe in het bijzonder de grondrechten op het gebied van vrijheid van meningsuiting gewaarborgd worden en, óf en hoe, voorkomen wordt dat door maatregelen van de Europese Commissie sprake kan zijn van vormen van censuur?

b. Vragen met betrekking tot COM(2025)837 – Omnibus Digitaal

De leden van de PVV-fractie lezen in het voorstel van de Omnibus Digitaal: *"De in deze verordening voorgestelde wijzigingen zullen een centraal toegangspunt invoeren die entiteiten in staat stelt tegelijkertijd aan hun verplichtingen inzake de melding van incidenten uit hoofde van meerdere rechtshandelingen te voldoen. Door het beginsel "eenmalig melden, veelvoudig delen" te bevorderen, zal het centrale toegangspunt de administratieve lasten voor entiteiten verminderen en tegelijkertijd zorgen voor een doeltreffende en veilige informatiestroom over beveiligingsincidenten naar de in de respectieve wetgeving gedefinieerde ontvangers."*³²

5. Kunt u nader duiden wat precies wordt verstaan onder een 'centraal toegangspunt' en wat in dit kader bedoeld wordt met 'incidenten' en 'kwetsbaarheden' en hoe en door wie deze bepaald worden?

³⁰ COM(2025) 836, p. 2.

³¹ COM(2025) 836, p. 3.

³² COM(2025) 837, p. 9.



datum 24 februari 2026

ons kenmerk 179856

blad 21

5. Vragen en opmerkingen van de leden van de fractie van Volt

De leden van de fractie van **Volt** hebben kennisgenomen van het BNC-fiche voor de Omnibus Digitaal en de Omnibus AI en het BNC-fiche voor de Data Unie Strategie. Zij wensen daarover de volgende vragen te stellen.

1. De regering geeft in de BNC-fiches aan dat *impact assessments* ontbreken bij de Omnibus Digitaal, de Omnibus AI en de Data Unie Strategie en dat zij hierover bij de Europese Commissie opheldering zou vragen. Heeft u deze opheldering inmiddels gevraagd en gekregen van de Europese Commissie? Als er aanvullende informatie is verstrekt over de impact, bent u dan bereid om die met onze Kamer te delen?
2. De regering geeft in het BNC-fiche aan dat het ontbreken van de *impact assessment* het voor de regering moeilijk maakt om te beoordelen welke effecten de Omnibus Digitaal en de Omnibus AI zullen hebben op de verlaging van de regeldruk en op de fundamentele grondrechten en de nationale bevoegdheden. Bent u van mening dat de voorgestelde wijzigingen en de afwegingen die de Europese Commissie daarbij heeft gemaakt voldoende kunnen worden beoordeeld? Zo nee, van welke voorgestelde wijzigingen kunt u nu de impact op de fundamentele rechten of de doelmatigheid (nog) niet goed inschatten of afwegen?
3. Wanneer verwacht u de nog ontbrekende informatie over de impact van de verschillende wijzigingen bij de Europese Commissie te kunnen opvragen? Kunt u een aanvullende impactbeoordeling delen met onze Kamer?
4. De leden van de Volt-fractie lezen in het BNC-fiche dat de regering een risico ziet op meer politieke besluitvorming bij de uitvoering van de AVG, omdat de Omnibus Digitaal uitvoeringsbevoegdheden verschuift van de onafhankelijke nationale en Europese toezichthouder(s) naar de Europese Commissie. Wat zal de verdere inzet van de regering zijn met betrekking tot dit risico bij de behandeling van de Omnibus Digitaal? Denkt u dit risico te kunnen mitigeren? Zo ja, op welke wijze?
5. De regering geeft in het BNC-fiche aan dat zij de adviezen van de Europees Toezichthouder voor gegevensbescherming (EDPS) en van het Europees Comité voor gegevensbescherming (EDPB) wil betrekken bij haar beoordeling en inzet op de Omnibus Digitaal en de Omnibus AI. Deze adviezen zijn inmiddels verschenen. Kunt u aangeven of u de adviezen en de daarin geuite zorgen onderschrijft? Hoe zal de regering deze adviezen bij de verdere Nederlandse inzet betrekken?
6. De regering geeft in het BNC-fiche aan grote zorgen te hebben over het instellen van een Europees meldpunt. Hoe meent u bij de behandeling van de Omnibus Digitaal te kunnen bereiken dat in plaats daarvan wordt voortgeborduurd op nationale meldpunten en oplossingen, zoals de regering in het BNC-fiche voorstaat?
7. De Omnibus Digitaal voorziet in een wijziging van de definitie van "persoonsgegevens". Onderschrijft u dat de voorgestelde wijziging leidt tot subjectiviteit en (rechts)onzekerheid met betrekking tot wanneer sprake is van persoonsgegevens en wanneer de AVG van toepassing is?
8. EDPB en EDPS uiten zorgen over het verruimen van het gebruik van bijzondere persoonsgegevens over bijvoorbeeld etniciteit of gezondheid voor het opsporen en



datum 24 februari 2026

ons kenmerk 179856

blad 22

corrigeren van discriminatie in AI-systemen.³³ Deelt u de opvatting van de Europese Commissie dat de bescherming tegen het gebruik van die gegevens in het huidige AI-landschap kan worden versoepeld? Zo ja, op basis waarvan komt u tot die conclusie? Wordt het risico op herleidbaarheid niet juist groter naarmate AI zich verder ontwikkelt, en blijft de bescherming daarom niet onverminderd noodzakelijk om directe of indirecte discriminatie te voorkomen? Op welke aanvullende waarborgen zet u in bij de verdere behandeling van de Omnibus Digitaal?

9. De Omnibus AI voorziet in het schrappen van de registratieplicht voor AI-systemen die aanbieders zelf niet aanmerken als hoog risico. Bent u bekend met de bezwaren die de toezichthouders AP en de EDPB hiertegen hebben geuit?³⁴ Deelt u de opvatting dat het schrappen van deze registratieplicht de transparantie en de uitvoerbaarheid van het toezicht vermindert? Op welke wijze betreft u de zorgen van de toezichthoudende instanties bij de verdere Nederlandse inzet ten aanzien van de Omnibus Digitaal en de Omnibus AI?
10. In het BNC-fiche heeft de regering zorgen geuit over de grondslag die in de Omnibus Digitaal wordt geïntroduceerd voor het verwerken van (bijzondere) persoonsgegevens. De regering geeft aan dat het belangrijk is dat er goede randvoorwaarden zijn. Welke randvoorwaarden moeten volgens u aanwezig zijn? Hoe zet de regering zich bij de behandeling van de Omnibus Digitaal in voor die randvoorwaarden?
11. De leden van de fractie van Volt constateren dat de regering een positieve houding inneemt ten aanzien van het voorstel van gecentraliseerde cookie-toestemming in de Omnibus Digitaal (art. 88ter). Voor digitale 'gatekeepers' onder de Digitale Markets Act (DMA) is dit begrijpelijk. Tegelijkertijd kan dit voorstel negatieve gevolgen hebben voor nieuwsuitgevers op de online advertentiemarkt en ook voor media dienstaanbieders. Op welke wijze wordt dit meegenomen bij de Nederlandse inzet? Bent u bereid voor beide een uitzonderingspositie te bedingen? In hoeverre acht u het risico aanwezig dat gecentraliseerde cookie-toestemming een oneigenlijk voordeel voor bepaalde delen van de digitale markt ten opzichte van andere delen daarvan?

6. Vragen en opmerkingen van het lid van fractie-Van de Sanden

Het lid van de fractie-Van de Sanden heeft kennisgenomen van het BNC-fiche voor de Omnibus Digitaal en de Omnibus AI en het BNC-fiche voor de Data Unie Strategie. De vragen van het lid van de fractie-**Van de Sanden** zijn opgesteld vanuit een liberaal perspectief met bijzondere aandacht voor de rechtsstaat, proportionaliteit, bescherming van grondrechten, administratieve lasten en het behoud van nationale beleidsruimte.

a. Rechtsstaat en democratische controle

³³ EDPB-EDPS Joint Opinion 1/2026 On the Proposal for a regulation as regards the simplification on the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI).

³⁴ Autoriteit Persoonsgegevens, 'Position paper AP: Omnibus Digitaal en Omnibus AI', 13 januari 2026, <https://www.autoriteitpersoonsgegevens.nl/documenten/position-paper-ap-omnibus-digitaal-en-omnibus-ai>;

EDPB-EDPS Joint Opinion 1/2026 On the Proposal for a regulation as regards the simplification on the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI).



datum 24 februari 2026

ons kenmerk 179856

blad 23

1. Kunt u uiteenzetten hoe u voorkomt dat de Omnibus Digitaal leidt tot een verdere verschuiving van bevoegdheden van nationale naar Europese toezichthouders zonder adequate democratische controle? Welke concrete waarborgen worden ingebouwd om te verzekeren dat de rol van nationale parlementen niet wordt gemarginaliseerd?

b. Proportionaliteitstoets

2. Welke proportionaliteitstoets heeft u uitgevoerd met betrekking tot de afzonderlijke onderdelen van de Omnibus Digitaal en de Omnibus AI? Kunt u per voorgestelde maatregel aangeven waarom deze noodzakelijk is, welk probleem wordt opgelost en waarom een minder ingrijpend alternatief niet volstaat?

c. Effect op administratieve lasten

3. Op welke wijze heeft u in kaart gebracht welke administratieve lastenreductie de Omnibus Digitaal daadwerkelijk oplevert voor Nederlandse bedrijven, in het bijzonder voor het midden- en kleinbedrijf en start-ups? Kunt u een concrete kosten-batenanalyse delen?

d. Grondrechten en AI-regulering

4. Hoe waarborgt u dat de aanpassingen in de Omnibus AI, waaronder uitstel van bepaalde verplichtingen uit de AI-verordening, niet leiden tot een verzwakking van de bescherming van fundamentele rechten zoals privacy, gelijke behandeling en het recht op effectieve rechtsbescherming?

e. Nationale beleidsruimte

5. In hoeverre beperken deze voorstellen de ruimte voor Nederland om eigen keuzes te maken op het terrein van digitalisering en AI-toepassingen? Kunt u aangeven welke onderdelen leiden tot volledige harmonisatie en waar nog nationale beleidsvrijheid resteert?

f. Toezicht en rechtsbescherming van burgers en bedrijven

6. Welke mogelijkheden blijven voor burgers en bedrijven bestaan om besluiten van Europese digitale toezichthouders aan te vechten bij een onafhankelijke rechter? Acht u deze rechtsbescherming toereikend. Zo ja, op grond waarvan?

g. Subsidiariteit en Europees meldpunt

7. De regering plaatst in het BNC-fiche een kanttekening bij het voorgestelde Europese meldpunt voor rapportageverplichtingen. Kunt u nader toelichten waarom desondanks geen formeel subsidiariteitsbezwaar wordt overwogen? Welke meerwaarde ziet u in dit meldpunt ten opzichte van nationale voorzieningen?

h. Gevolgen voor innovatie en concurrentievermogen

8. Hoe beoordeelt u de risico's dat de stapeling van Europese digitale regelgeving – waaronder de Omnibus Digitaal en de Omnibus AI – het Nederlandse innovatieklimaat kan verzwakken? Welke concrete maatregelen neemt u om te voorkomen dat compliance-eisen innovatie ontmoedigen?



datum 24 februari 2026

ons kenmerk 179856

blad 24

i. Digitale soevereiniteit en strategische autonomie

9. Hoe verhouden de voorstellen zich tot het streven naar behoud van Nederlandse en Europese digitale soevereiniteit? Kunt u aangeven op welke punten strategische beslissingsmacht feitelijk uit nationale handen wordt overgedragen en hoe dit wordt gewogen?

De leden van de vaste commissies voor Digitalisering en Economische Zaken & Klimaat en Groene Groei zien met belangstelling uit naar uw antwoorden en ontvangen deze graag **uiterlijk de vrijdag voorafgaand aan het mondeling overleg over het parlementair behandelvoorbehoud.**

Hoogachtend,

De voorzitter van de commissie Digitalisering
G. Veldhoen

De voorzitter van de commissie Economische Zaken & Klimaat en Groene Groei
S.M. Kluit

From: "Mary Fiers"
Sent: Sat, 4 Apr 2026 06:22:50 +0200
To: "5.1.2.e" <5.1.2.e@eerstekamer.nl>; "Cees van de Sanden" <cees.vandesanden@eerstekamer.nl>
Cc: "5.1.2.e" <5.1.2.e@eerstekamer.nl>; "5.1.2.e" <5.1.2.e@eerstekamer.nl>
Subject: RE: Advies TCGCT over omnibussen AI en Digitaal

Dank!

Hartelijke groeten,

Mary Fiers

Senator

Woordvoerder Binnenlandse Zaken en digitalisering



Van: 5.1.2.e <5.1.2.e@eerstekamer.nl>
Verzonden: vrijdag 3 april 2026 10:45
Aan: Mary Fiers <mary.fiers@eerstekamer.nl>; Cees van de Sanden <cees.vandesanden@eerstekamer.nl>
CC: 5.1.2.e <5.1.2.e@eerstekamer.nl>; 5.1.2.e <5.1.2.e@eerstekamer.nl>
Onderwerp: FW: Advies TCGCT over omnibussen AI en Digitaal

5.1.2.e

5.2,1

5.2,1

Met vriendelijke groet,

5.1.2.e

Stafmedewerker

Eerste Kamer *der Staten-Generaal*

Kazernestraat 52

Postbus 20017

2500 EA Den Haag

T 5.1.2.e

E 5.1.2.e [@eerstekamer.nl](mailto:5.1.2.e@eerstekamer.nl)

Van: 5.1.2.e <5.1.2.e@eerstekamer.nl>

Verzonden: Donderdag, 2 April, 2026 15:33

Aan: 5.1.2.e <5.1.2.e@eerstekamer.nl>; 5.1.2.e <5.1.2.e@eerstekamer.nl>; 5.1.2.e

5.1.2.e <5.1.2.e@eerstekamer.nl>

CC: 5.1.2.e <5.1.2.e@eerstekamer.nl>

Onderwerp: Advies TCGCT over omnibussen AI en Digitaal

Hoi 5.1.2.e 5.1.2.e en 5.1.2.e

Het advies van de TCGCT is binnen voor de TK commissie DiZa, zie hieronder:

Hartelijke groet,

5.1.2.e

Van: 5.1.2.e <5.1.2.e@tweedekamer.nl> 5.1.2.e <5.1.2.e@tweedekamer.nl>

Verzonden: donderdag 2 april 2026 15:01

Aan: 5.1.2.e <5.1.2.e@eerstekamer.nl>

Onderwerp: Vaste commissie voor Digitale Zaken op Tweede Kamer



Vaste commissie voor Digitale Zaken

Brief van de tijdelijke commissie Grondrechten en Constitutionele toetsing over een advies op verzoek van de vaste commissie voor Digitale Zaken over EU-voorstel: Verordening Digitale Omnibus AI COM (2025) 836 - Nieuwe Commissievoorstellen en initiatieven van de lidstaten van de Europese Unie

02-04-2026 | Brief van de tijdelijke commissie Grondrechten en Constitutionele toetsing over een advies op verzoek van de vaste commissie voor Digitale Zaken over EU-voorstel: Verordening Digitale Omnibus AI COM (2025) 836 -

Nieuwe Commissievoorstellen en initiatieven van de lidstaten van de Europese Unie. Brief van de tijdelijke commissie Grondrechten en

Brief van de tijdelijke commissie Grondrechten en Constitutionele toetsing over een advies op verzoek van de vaste commissie voor Digitale Zaken over EU-voorstel: Verordening Digitale Omnibus COM (2025) 837 - Nieuwe Commissievoorstellen en initiatieven van de lidstaten van de Europese Unie

02-04-2026 | Brief van de tijdelijke commissie Grondrechten en Constitutionele toetsing over een advies op verzoek van de vaste commissie voor Digitale Zaken over EU-voorstel: Verordening Digitale Omnibus COM (2025) 837 - Nieuwe Commissievoorstellen en initiatieven van de lidstaten van de Europese Unie. Brief van de tijdelijke commissie Grondrechten en

U ontvangt deze e-mail omdat u zich heeft geabonneerd op een zoekvraag op www.tweedekamer.nl.

Wilt u geen e-mailattendingen meer ontvangen over deze zoekvraag? Klik dan [hier](#) om u af te melden.

Wilt u helemaal geen e-mailattendingen meer ontvangen? Klik dan [hier](#) om u af te melden.

Of beheer [hier](#) al uw e-mailattendingen.

Voor vragen over onze attenderingservice kunt u een bericht sturen naar attendingen@tweedekamer.nl.

© 2026 Tweede Kamer der Staten-Generaal

From: "5.1.2.e"
Sent: 15-05-2026 17:52:29
To: "5.1.2.e" <5.1.2.e@eerstekamer.nl>; "5.1.2.e" <5.1.2.e@eerstekamer.nl>; "5.1.2.e" <5.1.2.e@eerstekamer.nl>
CC: "5.1.2.e" <Europapoort@eerstekamer.nl>; "5.1.2.e" <5.1.2.e@eerstekamer.nl>; "5.1.2.e" <5.1.2.e@eerstekamer.nl>; "5.1.2.e" <5.1.2.e@eerstekamer.nl>
Subject: RE: French Senate // PPRE avis motivé CSA2 et PPRE omnibus numérique
Attachments:

Dank 5.1.2.e

Dan is voor de staf digi met name de inhoud van de resolutie over de digitale omnibus mogelijk interessant om van op de hoogte te zijn.

5.1.2.e
Van: 5.1.2.e
Verzonden: vrijdag 15 mei 2026 17:47
Aan: 5.1.2.e ; 5.1.2.e ; 5.1.2.e ; 5.1.2.e
CC: 5.1.2.e ; 5.1.2.e ; 5.1.2.e ; 5.1.2.e
Onderwerp: RE: French Senate // PPRE avis motivé CSA2 et PPRE omnibus numérique

Bedankt 5.1.2.e!

5.2,1 5.1.2.e
5.2,1
5.2,1
5.2,1

Fijn weekend, groet,

5.1.2.e
Van: 5.1.2.e
Verzonden: woensdag 13 mei 2026 18:51
Aan: 5.1.2.e ; 5.1.2.e ; 5.1.2.e
CC: 5.1.2.e ; 5.1.2.e ; 5.1.2.e ; 5.1.2.e
Onderwerp: FW: French Senate // PPRE avis motivé CSA2 et PPRE omnibus numérique
Urgentie: Hoog

Hi collega's,

Zie bijgaand over de digitale omnibus en cybersecurity act.

Ik weet zo snel niet of cybersecurity is opgepakt en in welke commissie, dus ik zet collega's van J&V in cc bij.
Groet,

5.1.2.e
Van: 5.1.2.e
Verzonden: woensdag 13 mei 2026 18:02
Onderwerp: French Senate // PPRE avis motivé CSA2 et PPRE omnibus numérique

Dear colleagues,

At its meeting on May 13, the French Senate Committee on European Affairs adopted a reasoned opinion on the so-called "Cybersecurity Act 2" (CSA2) package (COM 2026 11 et 13 final) and an information report and a draft European resolution on the omnibus simplification package for the digital sector (COM 2025 836 et 837 final), presented by the European Commission on November 11, 2025.

Please find attached a summary in french and english

Best regards

5.1.2.e

--

5.1.2.e

Conseiller/Senior Adviser

Représentant administratif du Sénat français auprès des institutions européennes/French Senate office to the European institutions Paris : + 33 (0)1 42 34 37 44 – Mobile : + 5.2.1 (5.2.1 5.2.1 5.2.1 5.2.1 5.2.1) Bruxelles : PE + 32 2 284 38 27 – RP : + 32 2 229 82 07 e-mail : 5.1.2.e @senat.fr

| AVANT D'IMPRIMER, PENSEZ A L'ENVIRONNEMENT.

From: "Gala Veldhoen"
Sent: Mon, 18 May 2026 18:32:43 +0200
To: "5.1.2.e" <5.1.2.e@eerstekamer.nl>
Cc: "5.1.2.e" <5.1.2.e@eerstekamer.nl>; "5.1.2.e" <5.1.2.e@eerstekamer.nl>
Subject: Re: Gesprekspunten overleg rapporteurs

Dag 5.1.2.e

Dank, ik zat in overleg en zie je mail nu net. Memo lijkt me helder vanuit de staf en zie een voorstel voor de afspraak graag verschijnen.

Groet en tot morgen!

5.1.2.e

Op 18 mei 2026 om 15:56 heeft 5.1.2.e 5.1.2.e 5.1.2.e <5.1.2.E@eerstekamer.nl> het volgende geschreven:

Beste Gala,

5.1.2.E

5.2.1

Dan zet ik het door naar Mary en Cees. Het secretariaat is bezig een overleg in te plannen na dinsdag.

Graag tot morgen.

Hartelijke groet,

5.1.2.e

5.2.1

From: "5.1.2.e"
Sent: Fri, 5 5.1.2.e 2026 10:51:07 +0200
To: "Cees van de Sanden" <cees.vandesanden@eerstekamer.nl>; "Mary Fiers" <mary.fiers@eerstekamer.nl>
Bcc: "5.1.2.e" <5.1.2.e@eerstekamer.nl>
Subject: antwoordbrief Europese Commissie op commissievragen omnibussen
Attachments: C_2026_3661_1_NL_ACT_part1_v3.docx
Importance: High

5.1.2.e en 5.1.2.e

Bijgevoegd treffen jullie een brief aan van de Europese Commissie in antwoord op vragen van de commissies DIGI+EZ/KGG over de omnibus AI en omnibus Digitaal. Er wordt onder meer ingegaan op het achterwege laten van effectbeoordelingen. 5.2,1

5.2,1

5.2,1

5.2,1 5.1.2.e 5.1.2.e

5.2,1

5.2,1

5.2,1

5.2,1

5.2,1

5.2,1

5.2,1

5.2,1

5.2,1

Met vriendelijke groet,

5.1.2.e

Plaatsvervangend griffier

(griffier commissie Digitalisering)

Eerste Kamer *der Staten-Generaal*
Kazernestraat 52 (kamer 137)

2514 CV Den Haag

Postbus 20017
2500 EA Den Haag

M 5.1.2.e
E 5.1.2.e [@eerstekamer.nl](mailto:5.1.2.e@eerstekamer.nl)
I www.eerstekamer.nl



EUROPESE COMMISSIE

*Brussel, 2.6.2026
C(2026) 3661 final*

Geachte voorzitters,

De Commissie dankt de Eerste Kamer voor haar advies over het voorstel voor een verordening van het Europees Parlement en de Raad tot wijziging van de Verordeningen (EU) 2024/1689 en (EU) 2018/1139 wat betreft vereenvoudiging van de uitvoering van geharmoniseerde regels inzake artificiële intelligentie (digitale omnibus inzake AI) (COM(2025) 836 final), het voorstel voor een verordening van het Europees Parlement en de Raad tot wijziging van de Verordeningen (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725 en (EU) 2023/2854 en de Richtlijnen 2002/58/EG, (EU) 2022/2555 en (EU) 2022/2557 wat betreft de vereenvoudiging van het digitale wetgevingskader, en tot intrekking van de Verordeningen (EU) 2018/1807, (EU) 2019/1150 en (EU) 2022/868 en Richtlijn (EU) 2019/1024 (digitale omnibus) (COM(2025) 837 final), en de mededeling van de Commissie aan het Europees Parlement en de Raad – Strategie voor de data-unie: openstelling van data voor AI (COM(2025) 835 final).

De Commissie zet zich ten volle in voor de agenda voor vereenvoudiging van de regelgeving en voor een doeltreffende handhaving van de Europese regels. Die agenda is opgesteld naar aanleiding van de doelstellingen op het gebied van concurrentievermogen van het Draghi-verslag van 2024, die recentelijk herhaald zijn in de conclusies van de Europese Raad van 19 maart 2026. De agenda wordt op geen enkele wijze door externe actoren beïnvloed.

De twee omnibusvoorstellen bevatten een reeks technische wijzigingen van een groot corpus van digitale wetgeving om de toepassing ervan te vereenvoudigen. De maatregelen vormen een evenwichtig pakket en zijn bedoeld om bedrijven onmiddellijk

*Mevrouw Gala Veldhoen
Voorzitter van de vaste commissie
voor Digitalisering
Postbus 20017
2500 EA Den Haag, Nederland*

*cc: Mevrouw Mei Li Vos
Voorzitter van de Eerste Kamer
Postbus 20017
2500 EA Den Haag, Nederland*

*Mevrouw Saskia Kluit
Voorzitter van de vaste commissie
voor Economische Zaken & Klimaat en Groene Groei
Postbus 20017
2500 EA Den Haag, Nederland*

verlichting te bieden, een hoog niveau van bescherming van de grondrechten te handhaven en de handhaving van de regels van de Unie te verbeteren. De Europese bedrijven – in het bijzonder die van het type midden- en kleinbedrijf – zijn uitvoerig geraadpleegd, en de Commissie heeft er vertrouwen in dat de maatregelen een reëel effect voor hen zullen hebben en de digitale soevereiniteit van Europa zullen vergroten. Op basis van haar analyse raamt de Commissie dat uiterlijk in 2029 minstens 5 miljard EUR aan kostenbesparingen voor bedrijven kan worden gerealiseerd, en ze rekent erop dat de medewetgevers ondersteunende analyses delen als ze aanvullende wijzigingen voorstellen die van invloed kunnen zijn op deze eerste beoordeling.

De strategie voor de data-unie, die op dezelfde dag is gepubliceerd, bevat ambitieuze maatregelen om de toegang tot hoogwaardige data voor de ontwikkeling van artificiële intelligentie (AI) in de hele EU open te stellen en een open maar assertieve aanpak van internationale datastromen in gang te zetten.

De Commissie neemt nota van de verschillende punten die in het advies aan de orde worden gesteld. Een algemeen punt van zorg betreft het ontbreken van een effectbeoordeling voor de verschillende voorstellen. Er is geen volledige effectbeoordeling uitgevoerd aangezien de voorgestelde wijzigingen technisch of gericht van aard zijn, waarvoor volgens de werkmethoden van de Commissie in zeer uitzonderlijke en gerechtvaardigde gevallen een afwijking kan worden toegestaan. De diensten van de Commissie hebben een erg uitgebreid werkdocument opgesteld en bij het voorstel gevoegd. Het omvat uitgebreide kwalitatieve en kwantitatieve beoordelingen van de maatregelen op basis van uitgebreid overleg, vooral met Europese bedrijven. Dat materiaal biedt de medewetgevers bewijsmateriaal en informatie om het belang van de verschillende wijzigingen te wegen en te beoordelen.

De Commissie wil ook graag ingaan op de vragen over de algemene verordening gegevensbescherming (AVG). Ze benadrukt dat de wijzigingen van de digitale omnibus dienen om een toekomstgericht en geharmoniseerd kader voor gegevensbescherming in de hele eengemaakte markt tot stand te brengen, waarbij doeltreffende bescherming wordt gewaarborgd met meer rechtszekerheid. De wijzigingen weerspiegelen hoe de technologie zich heeft ontwikkeld en houden verband met recente gerechtelijke uitspraken. Belangrijk is dat de voorgestelde wijzigingen in overeenstemming zijn met de risicogebaseerde aanpak van de AVG. Als zodanig zouden ze met name ten goede komen aan kleine marktdeelnemers, die doorgaans verwerkingsactiviteiten met een laag risico uitvoeren.

Wat in het bijzonder de aan de orde gestelde punten over de definitie van persoonsgegevens betreft, benadrukt de Commissie dat met het voorstel verschillende verduidelijkingen met betrekking tot dat begrip in de AVG verankerd worden. Die vloeien voort uit meerdere arresten van het Europees Hof van Justitie (met name de Gemeenschappelijke Afwikkelingsraad/Europese Toezichthouder voor gegevensbescherming) en veranderen volgens de Commissie het begrip op zich niet. De Commissie is van plan een geharmoniseerde interpretatie van het gebruik van gepseudonimiseerde gegevens in de hele eengemaakte markt te formuleren. Met

betrekking tot de daarmee samenhangende kwestie van de voorgestelde bevoegdheid van de Commissie om uitvoeringshandelingen voor pseudonimiseringstechnieken vast te stellen, is de Commissie van plan technische richtsnoeren te verstrekken om ondernemingen te ondersteunen met doeltreffende pseudonimisering. Dat zou de naleving vergemakkelijken voor kleinere marktdeelnemers in de hele eengemaakte markt.

Ten aanzien van de voorgestelde wijzigingen van geautomatiseerde individuele besluitvorming (artikel 22 van de AVG) herinnert de Commissie de Eerste Kamer eraan dat het doel is de administratieve lasten te verlichten en juridische duidelijkheid te verschaffen voor verwerkingen. Dit doet geen afbreuk aan het niveau van gegevensbescherming, en de Commissie merkt op dat het Europees Comité voor gegevensbescherming en de Europese Toezichthouder voor gegevensbescherming de doelstellingen van deze wijziging in hun gezamenlijk advies 2/2026 hebben verwelkomd.

Wat de verwerking van persoonsgegevens in het kader van de ontwikkeling en exploitatie van AI betreft, wordt in de voorgestelde wijzigingen rekening gehouden met de kenmerken van AI met het oog op de ondersteuning van het concurrentievermogen van de EU, zonder daarbij het niveau van bescherming van persoonsgegevens te verminderen. De wijzigingen introduceren een beperkte afwijking voor de incidentele verwerking van bijzondere categorieën persoonsgegevens, waarbij verwerkingsverantwoordelijken verplicht worden dergelijke gegevens waar mogelijk te vermijden en te verwijderen of gelijkwaardige waarborgen toe te passen als verwijdering onevenredig zou zijn. De wijzigingen zouden ook verduidelijken dat de verwerking van persoonsgegevens voor AI kan berusten op het gerechtvaardigde belang van de verwerkingsverantwoordelijke, mits er voldaan wordt aan alle voorwaarden voor de toepassing van die rechtsgrondslag uit hoofde van de AVG, aan de eisen voor meer transparantie en aan het onvoorwaardelijke recht van de betrokkene om bezwaar te maken tegen een dergelijke verwerking.

De Commissie neemt verder ook nota van de bezorgdheid over de gevolgen van gecentraliseerde consentinstellingen voor het medialandschap en is ingenomen met het feit dat de commissies van de Eerste Kamer het belang van de uitzondering voor de media in het voorstel erkennen. Ze benadrukt dat de waarborging van de onafhankelijkheid en pluriformiteit van de media in ons medialandschap een belangrijke prioriteit blijft. De voorwaarde van één klik is een belangrijke maatregel om moeheid bij het toestaan van cookies aan te pakken: gebruikers kunnen met één klik weigeren cookies toe te staan, zodat een dergelijke optie niet achter meerdere lagen verborgen zit. De Commissie benadrukt dat deze regel geen invloed heeft op de inkomstenmodellen die aanbieders van mediadiensten kiezen als ze mediadiensten aanbieden.

De Commissie erkent de bezorgdheid van de Eerste Kamer over het overstappen van de ene naar de andere clouddienst. De gerichte wijzigingen in het voorstel voor een digitale omnibus hebben een beperkt toepassingsgebied en doen geen afbreuk aan de doelstelling van de dataverordening om een open en concurrerende cloudmarkt te bevorderen. Bovendien valt de bepaling tot de volledige afschaffing van de overstapkosten buiten het toepassingsgebied van die wijzigingen en blijft ze van toepassing op alle aanbieders.

Wat betreft de vragen over de oprichting van een centraal meldpunt voor cyberincidenten op Europees niveau, wil de Commissie benadrukken dat het principe “eenmalig melden, veelvoudig delen” breed wordt gesteund door belanghebbenden omdat dit de lasten beduidend vermindert. Een centraal meldpunt voor incidenten is niet alleen bedoeld als instrument om de lasten voor bedrijven te verminderen, maar ook als een dwingende stimulans om ontoereikende rapportage van cyberincidenten aan te pakken en om de autoriteiten te helpen op tijd uitgebreide informatie over incidenten te ontvangen. Er wordt technisch werk verricht voor een veilige oplossing, waarbij de lidstaten nauw worden betrokken.

Voorts neemt de Commissie nota van de bezorgdheid van de Eerste Kamer over de voorgestelde intrekking van de platform-to-businessverordening (P2B-verordening). De Commissie herinnert eraan dat het regelgevingskader voor platforms sinds 2019 is verbeterd, met name dankzij de digitalediensten- en de digitalemarktenverordening. De intrekking van de P2B-verordening heeft als doel een laag regelgeving te schrappen, zodat de naleving gemakkelijker en de regelgeving en de kosten voor zowel onlineplatforms als zakelijke gebruikers eenvoudiger wordt.

De leden van de Eerste Kamer brengen ook verschillende punten in verband met de AI-omnibus ter sprake. De Commissie herinnert eraan dat de AI-omnibus is ontworpen als een gerichte vereenvoudiging en niet om de kerndoelstellingen van de AI-verordening terug te draaien. Het voorstel biedt een antwoord op praktische uitdagingen bij de uitvoering, waaronder vertragingen bij normen en bij de opstelling van de toezichtcapaciteit.

Die punten worden met de voorgestelde wijzigingen aangepakt. De voorgestelde aanpassingen, die over de hele AI-omnibus gespreid zijn, zijn bedoeld om ervoor te zorgen dat verplichtingen praktisch afdwingbaar zijn in plaats van dat ze het algemene niveau van bescherming verlagen. De voorgestelde wijzigingen over AI-geletterdheid zouden de lidstaten en de Commissie bijvoorbeeld een algemene verplichting opleggen om de AI-geletterdheid te bevorderen, terwijl voor exploitanten specifieke eisen zouden blijven gelden voor de opleiding van personeel en de beschikbaarheid van competenties voor bepaalde verplichtingen. Voor andere vereenvoudigingsvoorstellen blijven alle desbetreffende verantwoordingsmechanismen bestaan. Zo worden bij de schrapping van een van de registratieverplichtingen niettemin de relevante documentatie-eisen voor de betrokken exploitanten behouden, zodat de traceerbaarheid en de mogelijkheid voor de autoriteiten om de beoordeling van de exploitant te verifiëren, gewaarborgd blijven. Dankzij die wijzigingen wordt de uitvoering werkbaarder en evenrediger en blijft er een hoog niveau van bescherming van de gezondheid, de veiligheid en de grondrechten behouden. De Commissie staat steeds open voor een constructief gesprek over de beste manier om de resterende punten van zorg tijdens het wetgevingsproces aan te pakken.

Wat ten slotte de strategie voor de data-unie betreft, benadrukt de Commissie dat dataruimten een belangrijke beleidsprioriteit zijn. Binnenkort zullen nieuwe initiatieven gelanceerd worden op gebieden die cruciaal zijn voor de soevereiniteit en strategische autonomie van Europa, waaronder de defensiesector. De Commissie benadrukt ook dat

de in de strategie geschetste maatregelen ter ondersteuning van het delen van data er niet toe leiden dat de Europese burgers minder beschermd worden, maar veeleer het algemene data- en privacykader verbeteren. Tot slot merkt de Commissie op dat de samenwerking op het gebied van data veilig en betrouwbaar en in overeenstemming met de waarden en belangen van de EU moet zijn, onder meer door middel van waarborgen tegen datalekken en maatregelen ter bescherming van gevoelige data. Het begrip “gelijkgestemde partners”, zoals opgemerkt door de Eerste Kamer, wordt zodoende begrepen op een contextuele en beleidsspecifieke manier, waarbij wordt verwezen naar partners waarmee samenwerking kan worden nagestreefd op basis van deze gedeelde principes en doelstellingen.

De Commissie is verheugd over het politieke akkoord tussen het Europees Parlement en de Raad over de AI-omnibus van 7 mei 2026, dat moet leiden tot eenvoudigere regels en meer veiligheid voor zowel burgers als bedrijven. De Commissie is vastbesloten de medewetgevers verder te helpen bij de vaststelling van een evenwichtige en ambitieuze reeks vereenvoudigingsmaatregelen voor de digitale omnibus. Ze werkt ook aan de uitvoering van de eerste acties die in de strategie voor de data-unie zijn aangekondigd, waaronder de lancering van de eerste datalabs en de vaststelling van nieuwe steunmaatregelen om bedrijven te helpen de dataverordening na te leven. Tot slot zullen in het kader van de komende digitale geschiktheidscontrole en de wetgeving inzake digitale rechtvaardigheid van de Commissie de bredere inspanningen worden voortgezet om de Europese digitale wetgeving op alle regelgevingsgebieden te moderniseren.

De Europese Commissie hoopt dat zij met dit antwoord voldoende is ingegaan op de door de Eerste Kamer aan de orde gestelde punten en kijkt uit naar de verdere voortzetting van de politieke dialoog.

Met vriendelijke groet,

Henna Virkkunen

Uitvoerend vicevoorzitter

Maroš Šefčovič

Lid van de Commissie



Vergaderjaar 2025-2026

36 890

Digitaal pakket van de Europese Commissie COM(2025)835, COM(2025)836, COM(2025)837, COM(2025)838

W**VERSLAG VAN EEN SCHRIFTELIJK OVERLEG**

Vastgesteld 19 juni 2026

De vaste commissies voor Digitalisering¹ en voor Economische Zaken & Klimaat en Groene Groei² heeft schriftelijk overleg gevoerd met de staatssecretaris van Economische Zaken en Klimaat en de staatssecretaris van Justitie en Veiligheid over **het non-paper bij de Omnibus Digitaal**. Bijgaand brengt de commissie hiervan verslag uit. Dit verslag bestaat uit:

- De uitgaande brief van 22 mei 2026.
- De antwoordbrief van 18 juni 2026.

De griffier van de vaste commissie voor Digitalisering,

5.1.2.e

¹ Samenstelling:

Baumgarten (JA21), Beukering (Fractie-Beukering), Fiers (GroenLinks-PvdA), Van Gasteren (Fractie-Van Gasteren), Goossen (BBB), Hartog (Volt), Van Hattem (PVV), Janssen (SP), Kanis (D66), Lievense (BBB), Van Meenen (D66), Musa (VVD), Nicolai (PvdD), Van den Oetelaar (FVD), Panman (BBB) (ondervoorzitter), Petersen (VVD), Ramsodit (GroenLinks-PvdA), Recourt (GroenLinks-PvdA), Van Rooijen (50PLUS), Roovers (GroenLinks-PvdA), Van de Sanden (Fractie-Van de Sanden), Steenkamp (CDA), Talsma (ChristenUnie), Veldhoen (GroenLinks-PvdA) (voorzitter), Visseren-Hamakers (Fractie-Visseren-Hamakers), De Vries (SGP), Walenkamp (Fractie-Walenkamp)

² Samenstelling:

Van Aelst-den Uijl (SP), Van Ballekom (VVD), Baumgarten (JA21), Beukering (Fractie-Beukering), Bovens (CDA), Crone (GroenLinks-PvdA), Dessing (FVD), Van Gasteren (Fractie-Van Gasteren), Van der Goot (OPNL), Van Gurp (GroenLinks-PvdA), Holterhues (ChristenUnie), Karaaslan (D66), Kluit (GroenLinks-PvdA) (voorzitter), Kroon (BBB), Van Langen-Visbeek (BBB) (ondervoorzitter), Van Meenen (D66), Panman (BBB), Perin-Gopie (Volt), Petersen (VVD), Van Rooijen (50PLUS), Van de Sanden (Fractie-Van de Sanden), Schalk (SGP), Steenkamp (CDA), Straus (VVD), Van Strien (PVV), Thijssen (GroenLinks-PvdA), Visseren-Hamakers (Fractie-Visseren-Hamakers), Walenkamp (Fractie-Walenkamp)

BRIEF VAN DE VOORZITTERS DE VASTE COMMISSIES VOOR DIGITALISERING EN VOOR ECONOMISCHE ZAKEN & KLIMAAT EN GROENE GROEI

Aan staatssecretaris Justitie en Veiligheid, Rechtsbescherming en Gevangeniswezen

Den Haag, 22 mei 2026

De leden van de fracties van **GL-PvdA**, **SP** en **PvdD** hebben met belangstelling kennisgenomen van het non-paper dat het kabinet aan de Europese Commissie en de lidstaten heeft aangeboden. In dit non-paper pleit het kabinet ervoor uit de Omnibus Digitaal die verder gaan dan simplificatie te schrappen of waar nodig aan te passen.³ Over dit non-paper en de daaraan ten grondslag liggende afwegingen hebben deze leden een aantal vragen. Het lid van de **fractie-Van de Sanden** sluit zich bij deze vragen aan.

Allereerst vragen deze leden of het kabinet advies heeft gevraagd of gekregen van de Autoriteit Persoonsgegevens of het College voor de Rechten van de Mens over de in het non-paper voorgestelde aanpak. Zo ja, kunt u deze reacties aan de Eerste Kamer beschikbaar stellen?

Deze leden lezen dat het kabinet voorstelt de “meest omstreden artikelen” uit de Omnibus Digitaal te schrappen. Kunt u toelichten op basis van welk afwegingskader of welke onderliggende argumentatie wordt voorgesteld om sommige artikelen uit de Omnibus Digitaal wel te schrappen en andere niet? Is er steun voor dit voorstel? Zo ja, van welke lidstaten? Moeten de artikelen die het kabinet voorstelt te schrappen geheel van tafel, of kunnen deze in aangepaste vorm alsnog onderdeel worden van de Omnibus Digitaal? Deze leden ontvangen graag een toelichting.

De omschrijving “meest omstreden artikelen” suggereert dat er ook “minder omstreden artikelen” zijn waarvan het kabinet niet voorstelt deze te schrappen. Kunt u aangeven welke artikelen het kabinet als “minder omstreden” beschouwt? Deze leden ontvangen graag per artikel een toelichting waarom het kabinet deze artikelen in de Omnibus Digitaal wenst te behouden.

Deze leden constateren dat het kabinet voorstelt om enkele artikelen waarop in een eerdere fase stevige kritiek is geuit door onder meer de Autoriteit Persoonsgegevens en het College voor de Rechten van de Mens, toch in de Omnibus Digitaal te behouden. Dit betreft bijvoorbeeld het vervallen van het algemene verbod op geautomatiseerde besluitvorming van artikel 22 lid 1 AVG en de beperking van het inzagerecht van artikel 15 AVG. Waarom is hiervoor gekozen? Deze leden ontvangen graag een toelichting.

Het kabinet stelt voorts in het non-paper voor om enkele artikelen van de Omnibus Digitaal te wijzigen. Kunt u aangeven welke wijzigingen precies worden voorgesteld en wat de impact van deze wijzigingen is? Is er steun voor deze voorstellen? Zo ja, van welke lidstaten? Deze leden ontvangen graag een toelichting.

De vaste commissies voor Digitalisering en Economische Zaken / Klimaat en Groene Groei zien met belangstelling uit naar uw reactie en ontvangen deze graag binnen vier weken na dagtekening van deze brief.

³ Kamerstukken I 2025/26, 36 890, nr. P.

De voorzitter van de commissie Digitalisering
G.V.M. Veldhoen

De voorzitter van de commissie Economische Zaken & Klimaat en Groene Groei
S.M. Kluit

BRIEF VAN DE STAATSSECRETARIS VAN ECONOMISCHE ZAKEN EN KLIMAAT EN DE STAATSSECRETARIS VAN JUSTITIE EN VEILIGHEID

Aan de Voorzitter van de Eerste Kamer der Staten-Generaal

Den Haag, 18 juni 2026

Sinds de publicatie van het Commissievoorstel op 11 november jl. wordt in de Raad onderhandeld over de Omnibus Digitaal. De Raadsonderhandelingen bevinden zich nu in een afrondende fase. Het Cypriotische voorzitterschap is voornemens om tijdens de Coreper-II-bespreking van 26 juni aanstaande het compromis dat zij dan verwachten te hebben bereikt aan de lidstaten voor te leggen en een mandaat te vragen voor de onderhandelingen met het Europees Parlement (EP). Middels deze brief informeren wij, mede namens de Minister van Justitie en Veiligheid, de Minister van Binnenlandse Zaken en Koninkrijksrelaties en de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties, uw Kamer conform de gemaakte informatie-afspraken over de ontwikkelingen in de onderhandelingen en hoe deze zich verhouden tot de kabinetsinzet zoals beschreven in het BNC-fiche. Het krachtenveld rond het voorstel is nog volop in beweging en over een aantal belangrijke onderdelen is nog discussie in de Raad. Daardoor kan het beoogde compromis in deze laatste fase nog op belangrijke onderdelen wijzigen. Middels deze brief geven wij uw Kamer een zo goed mogelijk beeld van de stand van zaken op het moment van schrijven. Deze stand van zaken zal de komende dagen waarschijnlijk voortdurend aan verandering onderhevig zijn. Er kunnen nog geen definitieve conclusies worden getrokken over de inhoud van het uiteindelijke compromis en daarmee ook niet over het oordeel hierover door het kabinet.

Middels deze brief gaan wij ook in op de schriftelijke vragen die de fracties van GL-PvdA, SP en PvdD 22 mei jl. hebben ingediend over het non-paper over de AVG-onderdelen van de Omnibus. Verder wordt met deze brief gevolg gegeven aan de toezegging uit het Mondeling Overleg van 26 mei jl. om nader in te gaan op het Nederlandse non-paper m.b.t. AVG-bepalingen en in het bijzonder de vraag in hoeverre hiervoor steun is en wat het krachtenveld is.

Europees centraal meldpunt

Voor wat betreft het Europees meldpunt voor incidentmeldingen lijkt er een meerderheid van de lidstaten te steunen dat in lijn met de Nederlandse inzet de nationale meldstructuren blijven behouden en er een Europees centraal informatiepunt komt, zoals ook bepleit in het non-paper hierover dat met uw Kamer is gedeeld⁴. Ook lijkt er steun te zijn voor een verplichting aan lidstaten om een nationaal centraal meldpunt in te richten. Het kabinet kan dit steunen, maar acht het hierbij wel van groot belang dat er voldoende flexibiliteit blijft om dit meldpunt in te richten op een manier die aansluit bij de bestaande nationale inrichting van meldstructuren. Hier blijft het kabinet zich in de laatste fase van de Raadsonderhandelingen voor inzetten.

Platform-to-Business(P2B)-verordening

Er lijken voldoende lidstaten te steunen dat in lijn met de kabinetsinzet bepaalde onderdelen van de Platform-to-Business(P2B)-verordening in stand blijven, zodat ondernemers die zakendoen op platforms op hetzelfde niveau beschermd blijven.

Datawetgeving

Over de voorgestelde wijzigingen van de datawetgeving was het kabinet bij het oorspronkelijke voorstel al grotendeels positief. Het Raadscompromis zal waarschijnlijk niet fundamenteel afwijken van de voorgestelde wijzigingen in het Commissievoorstel. Er lijkt onvoldoende steun om in lijn met de kabinetsinzet de bepalingen over data-altruïstische diensten en het opvragen van gegevens in noodsituaties te verwijderen. Het kabinet is positief dat er in ieder geval steun lijkt om deze bepalingen te versimpelen en verduidelijken.

⁴ Kamerstukken II 2025/2026, 22 112, nr. 4287

Er is nog discussie in Raad over de gewijzigde bepalingen die het mogelijk maken datadeling te weigeren als er risico's zijn op inbreuk op bedrijfsgeheimen. Het kabinet is positief over het Commissievoorstel op dit onderdeel en kan verdere verduidelijking van de bepalingen steunen. Het kabinet vindt het hierbij wel belangrijk dat er geen fundamentele wijzigingen worden gedaan en dat de verplichting om het weigeren van datadeling te onderbouwen en melden bij de toezichthouder blijft behouden.

AVG

Zoals uiteengezet in het BNC-fiche bij de Omnibus Digitaal (12 december 2025), is de Nederlandse inzet bij de Omnibusvoorstellen erop gericht om regelgeving te verduidelijken en stroomlijnen, terwijl de doelen van de wetgeving overeind blijven. De kabinetsinzet is daarom om voorstellen die verder gaan dan het verduidelijken, versimpelen en stroomlijnen te laten schrappen of door aanpassing, waar mogelijk en opportuun, aanvaardbaar te maken. Het kabinet zet zich daarom in om de gewijzigde definitie van persoonsgegevens te schrappen, evenals een speciale bepaling van een grondslag gerechtvaardigd belang voor AI, het artikel over residuele verwerking van bijzondere persoonsgegevens in AI-context en de bevoegdheid van de Commissie om zelf regels op te stellen over wanneer er sprake is van persoonsgegevens (in relatie tot pseudonimisering).

Bepaalde voorstellen zijn minder of zelfs in het geheel niet problematisch, bijvoorbeeld omdat deze voorstellen geen of geen wezenlijke afbreuk doen aan de bescherming van persoonsgegevens en met gerichte en realistische aanpassingen aanvaardbaar kunnen worden gemaakt, en tegelijkertijd bijdragen aan het reduceren van de ervaren regeldruk. Gedacht kan worden aan de voorgestelde wijzigingen in de meldplicht datalekken, of het voorstel om uniforme Europese lijsten op te stellen van situaties waarin een gegevensbeschermingseffectenbeoordeling (DPIA) wel of niet verplicht is. Ook omtrent de regulering van cookies zijn er oplossingen mogelijk die geen afbreuk doen aan het niveau van gegevensbescherming. Mede dankzij de kritische opinie van de EDPB en EDPS, vindt de Nederlandse inzet op belangrijke punten weerklank in de Raad. Dit neemt niet weg dat het krachtenveld in beweging is, en dat het resultaat ook op voor Nederland essentiële onderwerpen die raken aan het grondrecht, zoals het begrip persoonsgegevens en gerechtvaardigd belang en cookies, nog niet is bereikt. In het vervolg van deze brief ga ik nader in op een aantal door het kabinet in de Raad gedane tekstwijzigingsvoorstellen.

Definitie wetenschappelijk onderzoek

Het kabinet heeft in de Raad voorgesteld om de door de Commissie voorgestelde definitie van wetenschappelijk onderzoek te schrappen of anders significant te wijzigen om aan de zorgen tegemoet te komen. In de ogen van het kabinet is deze definitie te breed geformuleerd en niet in lijn met EDPB-richtsnoeren (05/2020) en een EDPS-opinie (6 januari 2020). Ook de EDPB en EDPS zijn kritisch en hebben wijzigingsvoorstellen gedaan. Nederland steunt deze voorstellen in de onderhandelingen. In deze voorstellen wordt onder meer toegevoegd dat wetenschappelijk onderzoek moet worden uitgevoerd op een autonome en onafhankelijke wijze, en dat dit nieuwe wetenschappelijke kennis genereert of bestaande wetenschappelijke aanvult, volgens een methodologische en systematische aanpak die consistent is met de normen van het betreffende wetenschappelijke vakgebied. Ook wordt toegevoegd dat wetenschappelijk onderzoek verifieerbare en transparante resultaten produceert. Deze voorstellen lijken in de Raad weerklank te vinden.

Bijzondere persoonsgegevens in AI-context

De Commissie heeft voorgesteld om een uitzondering te maken op het verwerkingsverbod van bijzondere persoonsgegevens voor "residuele" bijzondere persoonsgegevens bij de ontwikkeling en de exploitatie van een AI-systeem of AI-model. Dit zijn bijzondere persoonsgegevens die, ondanks het nemen van strikte technische en organisatorische maatregelen om te voorkomen dat zij worden verwerkt, onbedoeld worden verwerkt. Nederland heeft voorgesteld om deze bepaling te schrappen. De EDPB en EDPS uiten in hun opinie over de Digitale Omnibus echter begrip voor de voorgestelde uitzondering voor AI op het verwerkingsverbod. Onder lidstaten lijkt op dit moment onvoldoende draagvlak voor het schrappen van de voorgestelde uitzondering. Nederland heeft daarom – voor het geval dat een meerderheid van de lidstaten deze uitzondering wil handhaven – tekstvoorstellen

gedaan ter verbetering van het voorstel. Volgens het Commissievoorstel is de gegevensverwerking toegestaan als het een 'disproportionele inspanning' vergt om de gegevens te verwijderen, of als dit onmogelijk is. Nederland heeft voorgesteld om de uitzondering bij disproportionele inspanning te schrappen en de gegevensverwerking te beperken tot gevallen waarin het 'technisch onmogelijk' is om de persoonsgegevens te verwijderen. Ook daarbuiten heeft Nederland tal van voorstellen gedaan om de reikwijdte van de uitzonderingen te reduceren. Het kabinet zal zich inspannen om het Raadscompromis zoveel mogelijk in lijn te brengen met de hierboven beschreven inzet en u informeren over het uiteindelijke compromis.

Misbruik van inzageverzoeken

Inzageverzoeken kunnen op grond van artikel 12(5) AVG worden afgewezen als deze "kennelijk ongegrond of buitensporig zijn, met name vanwege hun repetitieve karakter". In het Commissievoorstel is afwijzing daarnaast mogelijk bij "misbruik voor andere doeleinden dan de bescherming van zijn gegevens". Het kabinet ziet dat het Commissievoorstel kan leiden tot nieuwe onzekerheid over de reikwijdte van deze misbruikbepaling. Het kabinet is daarop kritisch, omdat onzekerheid het risico van een groter aantal juridische (klacht)procedures bij de toezichthouder met zich meebrengt. De EDPB en EDPS hebben voorgesteld om 'misbruik' te specificeren als "abusive intention", wat aansluit bij de jurisprudentie van het Hof van Justitie en richtlijnen van de EDPB. Het kabinet steunt dit voorstel. Ook onder diverse andere lidstaten lijkt hiervoor draagvlak.

Geautomatiseerde individuele besluitvorming

Het huidige artikel 22 AVG formuleert nadrukkelijk een "recht" om niet te worden onderworpen aan geautomatiseerde besluitvorming. Het Commissievoorstel tot wijziging van artikel 22 AVG verwijst niet langer naar een "recht" en bevat een limitatieve opsomming van gevallen waarin geautomatiseerde besluitvorming is toegestaan. Met deze voorgestelde wijziging is niet beoogd dat de voorwaarden voor geautomatiseerde besluitvorming worden gewijzigd. De AP en het College voor de Rechten van de Mens hebben desalniettemin kritiek geuit op deze herformulering, en ook de EDPB en de EDPS zijn in hun opinie over de Omnibus Digitaal kritisch over de voorgestelde wijziging, die rechtsonzekerheid in de hand kan werken. Nederland deelt deze zorg en steunt het voorstel in de opinie van EDPB en EDPS om het artikel niet te wijzigen zoals voorgesteld door de Commissie. Voor dit standpunt lijkt in de Raad op dit moment steun te zijn. Daarnaast steunt het kabinet het voorstel van EDPB en EDPS om in een overweging te verduidelijken dat de toets op 'noodzaak' inhoudt dat er geen andere even effectieve en minder ingrijpende middelen (geautomatiseerd of niet) beschikbaar mogen zijn voor de verwerkingsverantwoordelijke.

Commissiebevoegdheden

In het Commissievoorstel krijgt de Commissie de bevoegdheid om door middel van uitvoeringshandelingen bindende interpretaties te geven over pseudonimisering (en daarmee indirect over het begrip persoonsgegevens), gegevensbeschermingseffectbeoordelingen (in welke gevallen die verplicht zijn en het sjabloon) en de meldplicht datalekken (idem). Zoals in eerdere antwoorden op Kamervragen en in het BNC-fiche is toegelicht, is het kabinet niet overtuigd van de noodzaak om bevoegdheden van de onafhankelijke EDPB over te dragen aan de Commissie. Daarom heeft Nederland tekstvoorstellen gedaan om ervoor te zorgen dat de EDPB de bevoegdheid behoudt om richtlijnen over deze onderwerpen uit te vaardigen. Hoewel de onderhandelingen nog gaande zijn, lijken deze tekstvoorstellen weerklank te vinden bij andere lidstaten.

Gerechtvaardigd belang in AI-context

Nederland heeft bepleit om de door de Europese Commissie voorgestelde bepaling over de grondslag 'gerechtvaardigd belang' in geval van AI te schrappen. Op dit onderwerp is op dit moment veel beweging in de Raad. Nederland zet erop in deze bepaling niet te laten terugkeren als een overweging. Ook een overweging kan ten onrechte de indruk wekken dat de grondslag 'gerechtvaardigd belang' standaard aanwezig is bij AI. Een overweging mag geen afbreuk doen aan de voorwaarden voor gerechtvaardigd belang.

Diverse (technische) verbeteringen

Nederland heeft tal van tekstvoorstellen gedaan op technische punten of op het gebied van de wetgevingskwaliteit. Diverse voorstellen vinden weerklank in de Raad. Een concreet voorbeeld is de meldplicht datalekken, waarbij Nederland heeft voorgesteld om niet alleen een lijst te verplichten van omstandigheden die erop wijzen dat melding verplicht is, maar ook een lijst van omstandigheden ter verduidelijking van wanneer een melding niet verplicht is (artikel 33, zesde lid).

Vervolg

Zoals in deze brief beschreven lijkt het kabinet op verschillende belangrijke punten binnen de Raad op steun te kunnen rekenen. Tegelijk is onzeker of die steun behouden blijft en zijn er verschillende punten waar nog discussie over is. In de laatste fase van de Raadsonderhandelingen kan er nog veel veranderen. Het kabinet zal zich blijven inspannen om het Raadscompromis zoveel mogelijk in lijn te brengen met de hierboven beschreven inzet en u informeren over het uiteindelijke compromis.

W.J.M. Aerdts
Staatssecretaris van Economische Zaken en Klimaat

Claudia van Bruggen
Staatssecretaris van Justitie en Veiligheid

From: "5.1.2.e"
Sent: Tue, 23 5.1.2.e 2026 17:35:50 +0200
To: "5.1.2.e" <5.1.2.e@eerstekamer.nl>; "5.1.2.e"
<5.1.2.e@eerstekamer.nl>; "5.1.2.e" <5.1.2.e@eerstekamer.nl>; "5.1.2.e"
<5.1.2.e@eerstekamer.nl>
Subject: FW: Kamerbrief aan de Eerste Kamer inzake beantwoording schriftelijke vragen inzake de inzet van de omnibusprocedure
Attachments: Beantwoording schriftelijke vragen inzake de inzet van de omnibusprocedure.docx, Beslisnota bi Beantwoording schriftelijke vragen inzake de inzet van de omnibusprocedure.pdf

Ter info

Van: 5.1.2.e
Verzonden: dinsdag 23 juni 2026 17:35
Aan: Cees van de Sanden <cees.vandesanden@eerstekamer.nl>
Onderwerp: FW: Kamerbrief aan de Eerste Kamer inzake beantwoording schriftelijke vragen inzake de inzet van de omnibusprocedure

Geachte heer Van de Sanden,

Bij dezen treft u de beantwoording aan van de gestelde schriftelijke vragen inzake de inzet van de omnibusprocedure.

Vriendelijke groet,

5.1.2.e 5.1.2.e

Van: 5.1.2.e <5.1.2.e@minbuza.nl>
Verzonden: dinsdag 23 juni 2026 16:59
Onderwerp: Kamerbrief aan de Eerste Kamer inzake beantwoording schriftelijke vragen inzake de inzet van de omnibusprocedure

Help save paper! 5.1.2.e you really need to print this email?

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.

This message may contain information that is not intended for you. If you are not the addressee or if this

message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

Ministerie van Buitenlandse Zaken

Aan de Voorzitter van de
Eerste Kamer der Staten-Generaal
Kazernestraat 52
Den Haag

**Ministerie van Buitenlandse
Zaken**

Rijnstraat 8
2515 XP Den Haag
Postbus 20061
Nederland

www.minbuza.nl

Onze referentie
BZ2628867

Uw referentie
181326U

Bijlage(n)
-

Datum 23 juni 2026
Betreft Beantwoording schriftelijke vragen inzake de inzet van de
omnibusprocedure

Geachte voorzitter,

Hierbij bied ik u, mede namens de minister van Economische Zaken en Klimaat, de antwoorden aan op de schriftelijke vragen gesteld door het lid Van de Sanden inzake de inzet van de omnibusprocedure. Deze vragen werden ingezonden op 2 juni 2026 met kenmerk 181326U.

De minister van Buitenlandse Zaken,

T.B.W. Berendsen

Antwoorden van de minister van Buitenlandse Zaken, mede namens de minister van Economische Zaken en Klimaat, op vragen van het lid Van de Sanden inzake de inzet van de omnibusprocedure

Ministerie van Buitenlandse Zaken

Onze referentie
BZ2628867

Vraag 1

Kan de minister bevestigen dat het ministerie van Buitenlandse Zaken, gelet op haar coördinerende verantwoordelijkheid voor EU-aangelegenheden, het aangewezen aanspreekpunt is voor vragen over het al dan niet gebruiken van omnibusprocedures door de Europese Commissie, de Raad en het Europese Parlement en het al dan niet daarbij uitvoeren van effectbeoordelingen ('Impact Assessments'), zoals door de staatssecretarissen 'Digitale Economie en Soevereiniteit' en 'Rechtsbescherming en Gevangeniswezen' tijdens het mondeling overleg d.d. 26 mei 2026 met de commissies Digitalisering en Economische Zaken en Groene Groei en de rapporteurs Van de Sanden en Fiers voor de Omnibussen AI en Digitaal is aangegeven?

Antwoord

Het ministerie van Buitenlandse Zaken vervult een coördinerende rol voor de verschillende omnibusvoorstellen, vanuit zijn brede verantwoordelijkheid voor de coördinatie van het Nederlandse standpunt ten aanzien van EU-aangelegenheden. Het ministerie van Economische Zaken en Klimaat is verantwoordelijk voor het beleid inzake betere regelgeving en daarmee voor de vormgeving van het Nederlandse standpunt over het gebruik van omnibusprocedures als instrument, inclusief het daarbij al dan niet uitvoeren van effectbeoordelingen. Daarom wordt deze beantwoording mede namens de minister van Economische Zaken en Klimaat verzonden.

Vraag 2

Deelt de minister de opvatting van de rapporteurs – in lijn met de standpunten hierover van door dezen geraadpleegde deskundigen - dat een omnibusprocedure naar haar aard uitsluitend is bedoeld voor technische consolidatie en vereenvoudiging van bestaande regels— derhalve voor 'vorm' en niet voor 'inhoud' — en dat het gebruik van een omnibusprocedure voor (wezenlijke) materiële wijzigingen zonder voorafgaande effectbeoordeling oneigenlijk is, te minder waar daarbij grondrechten aan de orde zijn? Kan de minister het standpunt van de regering toelichten.

Antwoord

Het kabinet verwelkomt de inzet van de Commissie om met omnibusvoorstellen en andere vereenvoudigingsinitiatieven onnodige regeldruk terug te dringen. Het aanpakken van onnodige regeldruk is, ook nationaal, voor het kabinet een prioriteit. Zoals benoemd in de beantwoording van de nadere vragen van de Eerste Kamer over de Omnibus Digitaal, Omnibus AI en Data Unie Strategie¹ van 22 mei jl., is de Nederlandse inzet bij de Omnibusvoorstellen in brede zin om regelgeving te verduidelijken en te stroomlijnen, terwijl de doelen van de wetgeving overeind blijven.

¹ Kamerstuk 36.890, EK, T

Een omnibusvoorstel wordt in de regel gebruikt om bestaande EU-regels te vereenvoudigen, te stroomlijnen, te consolideren of technisch aan te passen. De omnibusvoorstellen die sinds februari 2025 zijn gepresenteerd in het kader van de vereenvoudigingsopgaven beperken zich echter niet per definitie tot technische wijzigingen. Het kabinet heeft daartegen geen bezwaar mits eventuele inhoudelijke wijzigingen passen binnen de doelstelling om regelgeving eenvoudiger, duidelijker en beter uitvoerbaar te maken en de onderliggende beleidsdoelen overeind blijven.

Het kabinet acht het niet wenselijk dat impactvolle voorstellen zonder effectbeoordeling worden gepresenteerd. Het kabinet zal er daarom op blijven aandringen dat de Commissie bij impactvolle voorstellen, waaronder omnibusvoorstellen met significante effecten, een effectbeoordeling opstelt of overtuigend motiveert wanneer daarvan wordt afgezien.

Vraag 3

Bij welke omnibussen is er – behalve bij de digitale - in de afgelopen 2 jaar geen effectbeoordeling uitgevoerd?

Antwoord

Bij geen van de tien sinds 26 februari 2025 gepubliceerde omnibuspakketten heeft de Commissie een effectbeoordeling uitgevoerd.

Vraag 4

Hoe heeft de regering, in de Raad of langs andere weg, het ontbreken van effectbeoordelingen bij recente digitale omnibuspakketten aan de orde gesteld? De regering heeft eerder aangegeven herhaaldelijk en tevergeefs hiervoor te hebben gepleit; graag ontvang ik van u een feitelijk overzicht van dergelijke contacten – wanneer, in welke gremia, met welke lidstaten – en het resultaat ervan, in het bijzonder voor de Omnibus AI en de Digitale Omnibus.

Antwoord

Sinds de eerste bespreking van de Omnibus AI en de Digitale Omnibus in de Antici Group on Simplification op 21 november jl. heeft het kabinet herhaaldelijk gepleit voor het uitvoeren van een impact assessment. Dit heeft het kabinet zowel mondeling tijdens interventies in deze Raadswerkgroep gedaan, alsook via schriftelijk commentaar. Bovendien heeft het kabinet via het non-paper over de vergaande wijzigingen aan de Algemene Verordening Gegevensbescherming (AVG)² dat op 8 april jl. met uw Kamer gedeeld is bepleit dat wijzigingen die verder gaan dan de vereenvoudiging van regelgeving vergezeld zouden moeten zijn van een effectbeoordeling. In dat kader heeft het kabinet ook contact gezocht met gelijkgestemde lidstaten.

Ondanks de inspanningen van de regering is er onvoldoende steun in de Raad om de Commissie ertoe te zetten alsnog een effectbeoordeling uit te voeren. Voor wat betreft het resultaat van de bredere inzet voor de digitale omnibuspakketten bent u op 8 mei jl. geïnformeerd over de uitkomsten van de onderhandelingen over de

² Kamerstuk 36.890, EK, P

Omnibus AI.³ Het krachtenveld rondom de Omnibus Digitaal is nog in ontwikkeling. Er kan daarom nog niet worden geconcludeerd wat het resultaat is geweest van de Nederlandse inzet. Wel zijn er positieve signalen met betrekking tot het krachtenveld omtrent de belangrijkste zorgpunten van het kabinet.

Ministerie van Buitenlandse Zaken

Onze referentie
BZ2628867

Vraag 5

Is de minister bekend met de brief van het Committee of European Affairs van het Deense parlement ('Folketing') van 8 mei 2026 aan Eurocommissaris Dombrovskis, waarin op basis van haar eigen analyse — slechts 14 van de 64 belangrijke voorstellen vergezeld gingen van een effectbeoordeling — wordt aangedrongen op het terugkeren naar effectbeoordelingen als regel? Deelt de regering deze analyse en zo nee, waarom niet?

Antwoord

Ja, ik ben bekend met deze brief. Zoals benoemd in eerdere beantwoording deelt het kabinet de analyse dat de Commissie bij impactvolle voorstellen, waaronder omnibusvoorstellen met significante effecten, een effectbeoordeling zou moeten opstellen of overtuigend zou moeten motiveren wanneer daarvan wordt afgezien.

Vraag 6

Hoe weegt de regering de gezamenlijke opinie van de EDPB en de EDPS van 10 februari 2026 inzake de Digitale Omnibus, waarin beide toezichthouders betreuren dat een volledige effectbeoordeling ontbreekt en oordelen dat de mogelijke gevolgen voor de grondrechten onvoldoende zijn gewogen?

Antwoord

Zoals benoemd in eerdere beantwoording en onderstreept, betreurt het kabinet, net als het Europees Comité voor Gegevensbescherming (EDPB) en de Europese Toezichthouder voor Gegevensbescherming (EDPS), dat een volledige effectbeoordeling ontbreekt en dat de mogelijke gevolgen voor de grondrechten onvoldoende zijn gewogen.

Vraag 7

Hoe verhoudt zich volgens de regering de huidige inzet van de omnibusprocedure zonder effectbeoordelingen tot de Commissiemededeling "A Simpler, Clearer and Better Enforced EU Rulebook" (COM(2026) 380), waarin de Commissie zelf opnieuw committering aan betere regelgeving uitspreekt?

Antwoord

In de mededeling onderschrijft de Commissie het belang van effectbeoordelingen. De Commissie bevestigt in de mededeling het uitgangspunt dat ook voorstellen die gericht zijn op vereenvoudiging van bestaande regelgeving –zoals de omnibusvoorstellen- voorzien zouden moeten zijn van een effectbeoordeling. De Commissie geeft aan ervoor te willen zorgen dat deze voortaan in meer gevallen worden uitgevoerd.

³ Kamerstuk 36.890, EK, S

Vraag 8

Welke juridische weging maakt de regering, in het licht van rechtspraak van het Hof van Justitie van het risico dat onderdelen van Uniewetgeving die ten onrechte met gebruikmaking van onjuiste (omnibus)procedures en/of zonder benodigde effectbeoordeling tot stand komen op proportionaliteits- of andere gronden voor vernietiging in aanmerking kunnen komen?

Ministerie van Buitenlandse Zaken

Onze referentie
BZ2628867

Antwoord

Bij omnibuswetgeving worden meerdere bestaande Uniewetgevingshandelingen via één pakket Uniewetgeving gewijzigd. Het toepassen van een omnibusprocedure is op zichzelf genomen niet onrechtmatig. Hierbij wordt de procedure voor totstandkoming van Uniewetgeving zoals voorgeschreven door de EU-Verdragen doorlopen.

De Europese Commissie, Raad en het Europees Parlement zijn het er over eens dat effectbeoordelingen een positieve bijdrage leveren aan de verbetering van de kwaliteit van Uniewetgeving. Zij vormen een instrument dat de Uniewetgever helpt om tot goed onderbouwde besluiten te komen. Effectbeoordelingen zijn dan ook een stap in het wetgevingsproces die in de regel moet worden gezet zodra een wetgevingsinitiatief naar verwachting significante economische, ecologische of sociale gevolgen zal hebben.

Effectbeoordelingen zijn echter niet bindend voor de Uniewetgever, en treden niet in de plaats van de politieke besluiten van het democratische besluitvormingsproces. Ook volgt uit vaste rechtspraak van het EU Hof van Justitie dat er geen verplichting is om in alle omstandigheden een effectbeoordeling te verrichten.⁴ Meer in het bijzonder heeft het EU Hof geoordeeld dat het achterwege laten van een effectbeoordeling niet als een schending van het evenredigheidsbeginsel kan worden aangemerkt indien de Uniewetgever zich in een bijzondere situatie bevindt waardoor hij daarvan moet afzien en hij over voldoende gegevens beschikt om te beoordelen of een vastgestelde maatregel evenredig is.⁵ De Uniewetgever kan voor de beoordeling van de evenredigheid van de door hem vastgestelde maatregelen met elke andere informatiebron rekening houden,⁶ en heeft daarbij een ruime beoordelingsbevoegdheid.⁷

Het kabinet heeft dan ook geen aanleiding om te veronderstellen dat het enkele feit dat een omnibusprocedure wordt gevolgd zonder effectbeoordeling door de Europese Commissie reden is voor onrechtmatigheid van een door de Raad en het Europees Parlement vastgestelde verordening of richtlijn.

⁴ Arrest van 3 december 2019, Tsjechische Republiek/Parlement en Raad, C-482/17, EU:C:2019:1035, punt 82; arrest van 4 oktober 2024, Republiek Litouwen e.a./Parlement en Raad, gevoegde zaken C-541/20 tot en met C-555/20, ECLI:EU:C:2024:818, punt 221.

⁵ Arrest van 3 december 2019, Tsjechische Republiek/Parlement en Raad, C-482/17, EU:C:2019:1035, punten 84 en 85; arrest van 4 oktober 2024, Republiek Litouwen e.a./Parlement en Raad, gevoegde zaken C-541/20 tot en met C-555/20, ECLI:EU:C:2024:818, punt 225.

⁶ Arrest van 4 oktober 2024, Republiek Litouwen e.a./Parlement en Raad, gevoegde zaken C-541/20 tot en met C-555/20, ECLI:EU:C:2024:818, punt 220 en 600.

⁷ Arrest van 4 oktober 2024, Republiek Litouwen e.a./Parlement en Raad, gevoegde zaken C-541/20 tot en met C-555/20, ECLI:EU:C:2024:818, punt 219.

Dat neemt niet weg dat het kabinet het niet wenselijk acht dat impactvolle voorstellen zonder effectbeoordeling worden gepresenteerd. Het kabinet zal er daarom op blijven aandringen dat de Commissie bij impactvolle voorstellen, waaronder omnibusvoorstellen met significante effecten, een effectbeoordeling opstelt of overtuigend motiveert wanneer daarvan wordt afgezien.

Ministerie van Buitenlandse Zaken

Onze referentie
BZ2628867

Vraag 9

Is de regering bereid in de Raad, en waar passend jegens de Commissie, uitdrukkelijk stelling te nemen tegen het gebruik van de omnibusprocedure voor materiële wijzigingen zonder voorafgaande effectbeoordeling — niet alleen voor het lopende dossier Digitale Omnibus, maar als principieel uitgangspunt voor de overige aangekondigde omnibuspakketten voor zover dat daarin eveneens aan de orde zou kunnen zijn.

Antwoord

Zie het antwoord op vraag 2.

Vraag 10

Acht de regering een adviesvraag aan de Raad van State om voorlichting te geven over de juridische houdbaarheid van Uniewetgeving die via de omnibusprocedure zonder effectbeoordeling tot stand komt zinvol? Zo nee, waarom niet? Vragensteller ziet uw beantwoording – mede in het licht van de snelheid waarmee ernaar wordt gestreefd om de onderhandelingen over de Digitale Omnibus in de Raad ultimo juni 2026 af te ronden - graag binnen twee weken na heden met belangstelling tegemoet.

Antwoord

Met verwijzing naar het antwoord op vraag 8 ziet het kabinet geen meerwaarde in een adviesvraag om voorlichting van de Raad van State.



Aan
Van
Via
Kopie aan
Afgestemd met

M

Bescherming persoonlijke levenssfeer

TER BESLISSING

Datum

11 juni 2026

Onze referentie

BZ2628867

Opgesteld door

Bescherming persoonlijke levenssfeer

Uiterlijk bij

18 juni 2026

Binnengekomen op

2 juni 2026

Bijlage(n)

1

nota

Beantwoording vragen van het lid Van de Sanden op schriftelijke vragen inzake de inzet van de omnibusprocedure

Aanleiding

Schriftelijke vragen van het lid Van de Sanden (fractie-Van de Sanden) inzake de inzet van de omnibusprocedure en het ontbreken van effectbeoordelingen.

Geadviseerd besluit

Instemmen met de voorgestelde beantwoording van de schriftelijke vragen.

Kernpunten

- Op 2 juni jl. ontving u schriftelijke vragen van het lid Van de Sanden (fractie-Van de Sanden) inzake de inzet van de omnibusprocedure en het ontbreken van effectbeoordelingen.
- De vragen zien met name toe op de rechtmatigheid van het gebruik van omnibusprocedures en het uitblijven van effectbeoordelingen bij Commissievoorstellen.
- Deze beantwoording zal mede namens de Minister van Economische Zaken verstuurd worden.

Toelichting

- U vindt de beantwoording van de Kamervragen in de bijlage.
- Vanuit uw brede verantwoordelijkheid voor de coördinatie van het Nederlandse standpunt ten aanzien van EU-aangelegenheden heeft u samen met de Minister van Economische Zaken en Klimaat een gedeelde verantwoordelijkheid voor de Europese omnibusprocedures.
- Het lid Van de Sanden is de Eerste Kamer rapporteur voor het 'digitaal pakket', waar de Omnibus Digitaal en Omnibus AI onderdeel van uitmaken. In zijn hoedanigheid als rapporteur heeft hij eerder meermaals schriftelijke vragen en opmerkingen aan de staatssecretaris van EZ en van J&V over deze voorstellen gesteld.

Discussion Contribution AI Omnibus

Prepared by Prof. Dr. Natali Helberger, Institute for Information Law (IViR), University of Amsterdam

The envisaged AI Omnibus law entails a broad range of proposed changes, making a comprehensive discussion within the given constraints of time and the space difficult. In the spirit of the goal of the meeting – mapping the most important points of attention, potential risks and challenges – I will therefore flag several selected issues that from my perspective as legal scholar and expert in AI regulation require particular attention.

The Digital Omnibus on AI Regulation proposal

One important topic that so far has not received sufficient discussion are the proposed amendments to the **AI literacy obligations** under the AI Act. The European Commission itself has described AI literacy as central to the success of the Apply AI Strategy and the AI Continent Action Plan, and yet, the AI Omnibus proposes to scrape this legally binding obligation in favour of a mere “encouragement” and additional obligations for the Commission and member states. Taking away the obligation of providers and deployers of AI to invest in AI literacy is problematic for several reasons. First, the legal obligation requiring providers and deployers of AI to ensure a sufficient level of AI literacy among their staff is the only provision in the entire AI Act that protects society from incompetent AI use in so-called non-high-risk areas. Second, the proposed amendment would potentially also negatively affect employees and the need for continuous upskilling, as it removes the legal incentive for companies, especially smaller ones, to invest in staff training. The potential negative implications for long-term employability could be significant. Third, failure to invest in AI literacy and staff training will only deepen Europe’s dependency on US and Chinese AI companies that do invest heavily in expertise, which could have, fourth, negative repercussions for Europe’s digital autonomy. In the light of all these arguments, the proposed amendment is not simply a technical amendment, as the proposal itself claims (p.6), but a substantive amendment, and one with potentially important short- and long-term implications.

Second, there is paragraph 25 of the proposal that suggests that the supervision and enforcement of the compliance of GenAI systems embedded in designated very large online platforms or very large online search engines should fall under the sole competence of the AI Office. This proposal has the potential to create considerable legal uncertainty if it remains unclear what this means for the applicability of the provisions of the DSA. The relevance of this question becomes clear in the light of the considerations of the EC to classify ChatGPT as a Very Large Search Engine under the DSA. Were the DSA to apply to the use of GenAI embedded in VLOPS or VLOSEs, this would translate into additional regulatory oversight, public-facing transparency and expanding the focus of regulatory scrutiny to a broader set of issues than is currently the case under the AI Act. Examples are the potential application of Art. 40 DSA (researchers access to data), the transparency obligations under Article 15 but also more extensive risk management obligations under Art. 34 and 35 DSA. Hence, clarification is needed if in case AI systems embedded in VLOPs and VLOSEs fall under the authority

of the AI Office, the provisions of the DSA still apply and if there is a need for coordination with the EC as responsible for the enforcement of the relevant provisions in the DSA relating to VLOPs and VLOSEs.¹

Digital Omnibus Regulation proposal, as it relates to the GDPR

One of the proposed changes to the GDPR concerns narrowing down the definition of personal data that would fall under the GDPR by proposing that pseudonymised data would under certain conditions not be considered personal data (now it is). Also, the suggested changes to Art. 12 (5) of the GDPR, the right of citizens to access of their data, involve a substantive reduction of the right to data protection. The proposed amendment would allow controllers to refuse requests if used ‘for purposes other than the protection of their data’. Again, this is a substantive limitation of personal data protection law. As the ECJ has ruled, the right of access to data under the GDPR is not conditional upon a particular reason,² and indeed has already been instrumental in the realisation of other fundamental rights.³ Third, there is the proposal to allow the processing of personal data for the training of AI. These are three substantive changes to existing data protection law with potentially far-reaching implications for the right to data protection. An Omnibus law does not seem to be the right instrument for these interventions into fundamental rights, because of the lack of a proper impact assessment and limited public consultation and rule of law safeguards.⁴

Less often discussed but an important concern to take into account are the potential implications of the suggested changes to the GDPR for researchers and the right to academic freedom, including the freedom of research and a right of access to information, as a pre-condition for qualitative and reliable research.⁵ The proposed changes to Art. 12 (5) GDPR do not only limit the right to data protection of citizens but potentially also make impossible one of the few currently functioning instruments for researchers to access research data: data donations. Data donation research relies on citizens voluntarily sharing their data (obtained through access requests) to enable public interest research in a wide variety of fields, including on AI and platform-driven harms, impacts of digital technology on political polarisation, privacy and the realisation of fundamental rights. For these reasons, researchers across Europe have sounded the alarm about the restrictions of the right of access to information, and the negative consequences this can have for public interest innovation in Europe.⁶

¹ See also H. Graus, K. Karstka, N. Murali, J. Cave and M. Botterman, Interplay between the AI Act and the EU legislative framework, Study for the European Parliament, October 2025, [https://www.europarl.europa.eu/RegData/etudes/STUD/2025/778575/ECTI_STU\(2025\)778575_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2025/778575/ECTI_STU(2025)778575_EN.pdf)

² ECJ, Case C-307/22, FT vs DW, 26 October 2023, Para 38.

³ See the insightful analysis by R. Mahieu, The Omnibus Omnibus, Verfassungsblog, 3 December 2025.

⁴ See e.g. A. Alemanno, The Legality of Omnibus Legislation under EU Law: A Preliminary Analysis of Omnibus 1 Simplification Directive of CSRD and CSDD and its Legal Consequences on the EU Legal Order, HEC Paris Research Paper No. LAW-2025-1588, 9 November 2025, online available on https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5727822

⁵ LERU, Academic Freedom as a Fundamental Right, Advice Paper No. 6, December 2010, P. 12, online available at: <https://www.leru.org/files/Academic-Freedom-as-a-Fundamental-Right-Full-paper.pdf>

⁶ Datadonation.eu, Urgent Call to Reject the Omnibus Regulation with Regard to the GDPR's Right of Access, <https://datadonation.eu/community/omnibus-letter>

Potentially problematic from the perspective of the right to academic freedom and the effectiveness of the GDPR is also the proposed amended definition of “scientific research.” This amended definition clarifies that research may also pursue commercial objectives and defines research as “any research which can also support innovation, such as technological development or demonstration”. On the one hand, this framing of “any research which can also support innovation” can potentially exclude types of research that do not directly support innovation, even if it protected by academic freedom and scientific nature.⁷ The proposed change could make it impossible for e.g. research in the humanities or social sciences to benefit from the research exemptions in the GDPR.

On the other hand, the explicit reference to research for a commercial objective can potentially also be used by **commercial AI companies to circumvent safeguards GDPR. Large AI companies such as Open AI, Anthropic or Google explicitly position themselves as research-based, with the consequence that they could benefit from the research exemptions in the GDPR, even if the research is primarily profit driven. Such a wide interpretation of the research exemption could have the effect of exempting a significant share of AI companies from the obligations to perform compatibility assessment for data reuse (as research can qualify as legitimate interest), the GDPR information requirements, the purpose limitation requirements, enable them to benefit from exemptions when it comes to the processing of special categories of data as well as the right to rectification, without any of the obligations that apply to public interest research (like publication of research findings and adhering to professional research ethics).**

To avoid this situation, the EDPB-EDPS proposed to clarify that “scientific research should: 1. be conducted following a methodological and systematic approach of the relevant scientific research field. In addition, it should be added that scientific research should be conducted in an autonomous and independent manner;

2. lead to verifiable and transparent results. It is recommended to explain in the recitals that transparency may, among other things, involve making research results publicly available.”⁸

A general remark on deregulation and innovation

On a more general note, an underlying assumption under the Digital Omnibus is that simpler rules will promote innovation, economic growth and value for European citizens. More discussion is needed if the amendments will indeed stimulate economic growth (and whose), and what kind of innovation it must stimulate.⁹ If the goal is to stimulate innovation to address challenges and opportunities for the realisation of fundamental rights and principles that underpin European society (as envisaged e.g. in the EU Continent Action plan, p. 1), the proposed changes do little to incentivise public interest innovation or the safe and trustworthy deployment of AI in various societal and

⁷ This is a concern also shared e.g. by the EDPB-EDPS, EDPB-EDPS, Joint Opinion 2/2026 on the proposal for a regulation as regards the simplification of the digital legislative framework (Digital Omnibus), 10 February 2026, online available at: https://www.edpb.europa.eu/system/files/2026-02/edpb_edps_jointopinion_202602_digitalomnibus_en.pdf

⁸ Ibid, p. 13.

⁹ See e.g. the discussion on the potential economic benefits in L. Quaritsch, The EU’s Digital Omnibus is heading in the wrong direction, Policy Brief Hertie School, 30.03.2026, online available at: <https://www.delorscentre.eu/en/publications/detail/publication/the-eus-digital-and-ai-omnibus>

economic sectors in Europe. The proposed changes do not prioritise or benefit in particular AI developers that actively seek to further fundamental rights and European values, nor are they designed to explicitly benefit European companies. For example, one way to incentivise public interest innovation could be to limit the provisions in the AI Omnibus that allow real-world testing to innovation that is explicitly in the public interest, and Art. 57 (5) on sandboxes could be amended to speak of “public interest innovation” instead of innovation in general.

From the perspective of AI deployers and consumers, not de-regulation but legal certainty and a high level of protection for trustworthy AI that respects fundamental rights and public values may be indeed important to stimulate innovation. In that regard, the simplification and de-regulation agenda can undermine, rather than increase trust in AI, its wider deployment (as envisaged by the European AI Strategy), as well as the commitment of governments to protect the interests and fundamental rights of citizens.¹⁰

An overall risk of the proposal is that it contributes to legal uncertainty rather than taking legal uncertainty away due to its timing (companies, regulatory authorities and other relevant stakeholders are in the middle of implementing the AI Act when the rules change) and the lack of a proper impact assessment (because the rules of the AI Act are so new, and some have not even entered into force assessing the impact and challenges of the existing rules is difficult if not impossible). For these reasons, any significant substantive changes could be potentially more disruptive than helpful and would ideally be postponed after the envisaged digital fitness check in 2027.

10



Eerste Kamer der Staten-Generaal

Binnenhof 22
postbus 20017
2500 EA Den Haag

telefoon 070-312 92 00

e-mail postbus@eerstekamer.nl
internet www.eerstekamer.nl

datum 8 april 2026

betreft uitnodiging voor een gesprek met de rapporteurs over de Omnibus AI & Omnibus Digitaal

ons kenmerk 180566

Geachte 5.1.2.e

De vaste commissies voor Digitalisering en Economische Zaken & Klimaat en Groene Groei behandelen momenteel twee omvangrijke verordeningsvoorstellen van de Europese Commissie, namelijk de Omnibus Digitaal (COM(2025)837) en de Omnibus AI (COM(2025)836).

Vanwege de omvang en complexiteit van deze voorstellen heeft de Kamer besloten ondergetekenden tot rapporteurs te benoemen. Wij hebben tot taak om ten behoeve van voornoemde commissies informatie te vergaren die benut kan worden bij de behandeling van deze voorstellen. Daartoe willen wij in gesprek gaan met stakeholders en deskundigen om de belangrijkste aandachtspunten, risico's en mogelijke knelpunten in kaart te brengen. In de Eerste Kamer ligt de nadruk bij de behandeling van (Europese) wetsvoorstellen op de toetsing van rechtmatigheid, handhaafbaarheid en uitvoerbaarheid.

Graag nodigen wij u uit om van gedachten te wisselen over deze voorstellen. In het bijzonder zouden wij graag inzicht verkrijgen in de implicaties van de voorgestelde wijzigingen van de AI-verordening en de AVG, de samenhang met het bestaande wettelijke kader en de verwachte impact van de voorstellen op de bescherming van grondrechten, zoals het recht op privacy en gegevensbescherming.

Het gesprek zal circa één uur duren en vindt digitaal plaats. Wij stellen voor het gesprek te voeren op 28 april, van 13.00 tot 14.30. Het gesprek vindt plaats in een informele setting. De bijeenkomst zal niet worden uitgezonden via livestream. Wel wordt er een samenvattend verslag gemaakt dat als kamerstuk gepubliceerd zal worden.

Mevrouw Helberger en mevrouw Drechsler zijn tevens uitgenodigd voor dit gesprek.

Ter voorbereiding stellen wij het op prijs voorafgaand aan het gesprek een korte notitie te ontvangen, wanneer u daartoe in de gelegenheid bent, waarin u uw visie geeft op de belangrijkste aandachtspunten en eventuele risico's van de voorstellen.



datum 8 april 2026

ons kenmerk 180566

blad 2

Indien u bereid bent om deel te nemen, ontvangen wij graag uw reactie. Deze kunt u richten aan onze ondersteunende stafleden 5.1.2.e Deerstekamer.nl en 5.1.2.e @eerstekamer.nl.

Hoogachtend,

Drs. M.C.T. Fiers
Rapporteur

Mr. C.A.H. van de Sanden LL.M
Rapporteur



Eerste Kamer der Staten-Generaal

Binnenhof 22
postbus 20017
2500 EA Den Haag

telefoon 070-312 92 00

e-mail postbus@eerstekamer.nl
internet www.eerstekamer.nl

datum 8 april 2026

betreft uitnodiging voor een gesprek met de rapporteurs over de Omnibus AI & Omnibus Digitaal

ons kenmerk 180565

Geachte heer/mevrouw,

De vaste commissies voor Digitalisering en Economische Zaken & Klimaat en Groene Groei behandelen momenteel twee omvangrijke verordeningsvoorstellen van de Europese Commissie, namelijk de Omnibus Digitaal (COM(2025)837) en de Omnibus AI (COM(2025)836).

Vanwege de omvang en complexiteit van deze voorstellen heeft de Kamer besloten ondergetekenden tot rapporteurs te benoemen. Wij hebben tot taak om ten behoeve van voornoemde commissies informatie te vergaren die benut kan worden bij de behandeling van deze voorstellen. Daartoe willen wij in gesprek gaan met stakeholders en deskundigen om de belangrijkste aandachtspunten, risico's en mogelijke knelpunten in kaart te brengen. In de Eerste Kamer ligt de nadruk bij de behandeling van (Europese) wetsvoorstellen op de toetsing van rechtmatigheid, handhaafbaarheid en uitvoerbaarheid.

Graag nodigen wij u uit om van gedachten te wisselen over deze voorstellen. In het bijzonder zouden wij graag inzicht verkrijgen in de impact van deze voorstellen op de bescherming van grondrechten, zoals het recht op privacy en gegevensbescherming en non-discriminatie.

Het gesprek zal circa één uur duren en vindt digitaal plaats. Wij stellen voor het gesprek te voeren op 29 april, van 13.00 tot 14.00. Het gesprek vindt plaats in een informele setting. De bijeenkomst zal niet worden uitgezonden via livestream. Wel wordt er een samenvattend verslag gemaakt dat als kamerstuk gepubliceerd zal worden.

Het College voor de Rechten van de Mens en Bits of Freedom zijn tevens voor dit gesprek uitgenodigd.

Ter voorbereiding stellen wij het op prijs voorafgaand aan het gesprek een korte notitie te ontvangen, wanneer u daartoe in de gelegenheid bent, waarin u uw visie geeft op de belangrijkste aandachtspunten en eventuele risico's van de voorstellen.



datum 8 april 2026

ons kenmerk 180565

blad 2

Indien u bereid bent om deel te nemen, ontvangen wij graag uw reactie. Deze kunt u richten aan onze ondersteunende stafleden [5.1.2.e](#) @eerstekamer.nl en [5.1.2.e](#) @eerstekamer.nl.

Hoogachtend,

Drs. M.C.T. Fiers

Rapporteur

Mr. C.A.H. van de Sanden LL.M

Rapporteur



Eerste Kamer der Staten-Generaal

Kazernestraat 52
2514 CV Den Haag
postbus 20017
2500 EA Den Haag

telefoon 070 312 92 00
fax 070 312 93 90

e-mail postbus@eerstekamer.nl
internet www.eerstekamer.nl

datum 8 april 2026

betreft uitnodiging voor een gesprek met de rapporteurs over de Omnibus AI &
Omnibus Digitaal

ons kenmerk 180564

Geachte heer/mevrouw,

De vaste commissies voor Digitalisering en Economische Zaken & Klimaat en Groene Groei behandelen momenteel twee omvangrijke verordeningsvoorstellen van de Europese Commissie, namelijk de Omnibus Digitaal (COM(2025)837) en de Omnibus AI (COM(2025)836).

Vanwege de omvang en complexiteit van deze voorstellen heeft de Kamer besloten ondergetekenden tot rapporteurs te benoemen. Wij hebben tot taak om ten behoeve van voornoemde commissies informatie te vergaren die benut kan worden bij de behandeling van deze voorstellen. Daartoe willen wij in gesprek gaan met stakeholders en deskundigen om de belangrijkste aandachtspunten, risico's en mogelijke knelpunten in kaart te brengen. In de Eerste Kamer ligt de nadruk bij de behandeling van (Europese) wetsvoorstellen op de toetsing van rechtmatigheid, handhaafbaarheid en uitvoerbaarheid.

Graag nodigen wij u uit om van gedachten te wisselen over deze voorstellen. In het bijzonder zouden wij graag inzicht verkrijgen in huidige en de verwachte regeldruk voor bedrijven en de verwachte effecten ten aanzien van de concurrentiekracht en lastenverlichting.

Het gesprek zal circa één uur duren en vindt ofwel digitaal ofwel fysiek in de Eerste Kamer plaats. Wij stellen voor het gesprek te voeren op 28 april, van 15.00 tot 16.00. Het gesprek vindt plaats in een informele setting. De bijeenkomst zal niet worden uitgezonden via livestream. Wel wordt er een samenvattend verslag gemaakt dat als kamerstuk gepubliceerd zal worden.

Het Adviescollege Toetsing Regeldruk (ATR) is tevens voor dit gesprek uitgenodigd.



datum 8 april 2026

ons kenmerk 180564

blad 2

Ter voorbereiding stellen wij het op prijs voorafgaand aan het gesprek een korte notitie te ontvangen, wanneer u daartoe in de gelegenheid bent, waarin u uw visie geeft op de belangrijkste aandachtspunten en eventuele risico's van de voorstellen.

Indien u bereid bent om deel te nemen, ontvangen wij graag uw reactie. Deze kunt u richten aan onze ondersteunende stafleden 5.1.2.e@eerstekamer.nl en 5.1.2.e@eerstekamer.nl.

Hoogachtend,

Drs. M.C.T. Fiers
Rapporteur

Mr. C.A.H. van de Sanden LL.M
Rapporteur



Eerste Kamer der Staten-Generaal

Binnenhof 22
postbus 20017
2500 EA Den Haag

telefoon 070-312 92 00

e-mail postbus@eerstekamer.nl
internet www.eerstekamer.nl

datum 8 april 2026

betreft uitnodiging voor een gesprek met de rapporteurs over de Omnibus AI & Omnibus Digitaal

ons kenmerk 180565

Geachte heer/mevrouw,

De vaste commissies voor Digitalisering en Economische Zaken & Klimaat en Groene Groei behandelen momenteel twee omvangrijke verordeningsvoorstellen van de Europese Commissie, namelijk de Omnibus Digitaal (COM(2025)837) en de Omnibus AI (COM(2025)836).

Vanwege de omvang en complexiteit van deze voorstellen heeft de Kamer besloten ondergetekenden tot rapporteurs te benoemen. Wij hebben tot taak om ten behoeve van voornoemde commissies informatie te vergaren die benut kan worden bij de behandeling van deze voorstellen. Daartoe willen wij in gesprek gaan met stakeholders en deskundigen om de belangrijkste aandachtspunten, risico's en mogelijke knelpunten in kaart te brengen. In de Eerste Kamer ligt de nadruk bij de behandeling van (Europese) wetsvoorstellen op de toetsing van rechtmatigheid, handhaafbaarheid en uitvoerbaarheid.

Graag nodigen wij u uit om van gedachten te wisselen over deze voorstellen. In het bijzonder zouden wij graag inzicht verkrijgen in de impact van deze voorstellen op de bescherming van grondrechten, zoals het recht op privacy en gegevensbescherming en non-discriminatie.

Het gesprek zal circa één uur duren en vindt digitaal plaats. Wij stellen voor het gesprek te voeren op 29 april, van 13.00 tot 14.00. Het gesprek vindt plaats in een informele setting. De bijeenkomst zal niet worden uitgezonden via livestream. Wel wordt er een samenvattend verslag gemaakt dat als kamerstuk gepubliceerd zal worden.

Het College voor de Rechten van de Mens en Bits of Freedom zijn tevens voor dit gesprek uitgenodigd.

Ter voorbereiding stellen wij het op prijs voorafgaand aan het gesprek een korte notitie te ontvangen, wanneer u daartoe in de gelegenheid bent, waarin u uw visie geeft op de belangrijkste aandachtspunten en eventuele risico's van de voorstellen.



datum 8 april 2026

ons kenmerk 180565

blad 2

Indien u bereid bent om deel te nemen, ontvangen wij graag uw reactie. Deze kunt u richten aan onze ondersteunende stafleden [5.1.2.e](#) @eerstekamer.nl en [5.1.2.e](#) @eerstekamer.nl.

Hoogachtend,

Drs. M.C.T. Fiers
Rapporteur

Mr. C.A.H. van de Sanden LL.M
Rapporteur



Eerste Kamer der Staten-Generaal

Kazernestraat 52
2514 CV Den Haag
postbus 20017
2500 EA Den Haag

telefoon 070 312 92 00
fax 070 312 93 90

e-mail postbus@eerstekamer.nl
internet www.eerstekamer.nl

datum 8 april 2026

betreft uitnodiging voor een gesprek met de rapporteurs over de Omnibus AI &
Omnibus Digitaal

ons kenmerk 180564

Geachte heer/mevrouw,

De vaste commissies voor Digitalisering en Economische Zaken & Klimaat en Groene Groei behandelen momenteel twee omvangrijke verordeningsvoorstellen van de Europese Commissie, namelijk de Omnibus Digitaal (COM(2025)837) en de Omnibus AI (COM(2025)836).

Vanwege de omvang en complexiteit van deze voorstellen heeft de Kamer besloten ondergetekenden tot rapporteurs te benoemen. Wij hebben tot taak om ten behoeve van voornoemde commissies informatie te vergaren die benut kan worden bij de behandeling van deze voorstellen. Daartoe willen wij in gesprek gaan met stakeholders en deskundigen om de belangrijkste aandachtspunten, risico's en mogelijke knelpunten in kaart te brengen. In de Eerste Kamer ligt de nadruk bij de behandeling van (Europese) wetsvoorstellen op de toetsing van rechtmatigheid, handhaafbaarheid en uitvoerbaarheid.

Graag nodigen wij u uit om van gedachten te wisselen over deze voorstellen. In het bijzonder zouden wij graag inzicht verkrijgen in huidige en de verwachte regeldruk voor bedrijven en de verwachte effecten ten aanzien van de concurrentiekracht en lastenverlichting.

Het gesprek zal circa één uur duren en vindt ofwel digitaal ofwel fysiek in de Eerste Kamer plaats. Wij stellen voor het gesprek te voeren op 28 april, van 15.00 tot 16.00. Het gesprek vindt plaats in een informele setting. De bijeenkomst zal niet worden uitgezonden via livestream. Wel wordt er een samenvattend verslag gemaakt dat als kamerstuk gepubliceerd zal worden.

Het Adviescollege Toetsing Regeldruk (ATR) is tevens voor dit gesprek uitgenodigd.



datum 8 april 2026

ons kenmerk 180564

blad 2

Ter voorbereiding stellen wij het op prijs voorafgaand aan het gesprek een korte notitie te ontvangen, wanneer u daartoe in de gelegenheid bent, waarin u uw visie geeft op de belangrijkste aandachtspunten en eventuele risico's van de voorstellen.

Indien u bereid bent om deel te nemen, ontvangen wij graag uw reactie. Deze kunt u richten aan onze ondersteunende stafleden 5.1.2.e@eerstekamer.nl en 5.1.2.e@eerstekamer.nl.

Hoogachtend,

Drs. M.C.T. Fiers
Rapporteur

Mr. C.A.H. van de Sanden LL.M
Rapporteur

WHITE PAPER ON THE DIGITAL OMNIBUS PROPOSAL AND THE AI OMNIBUS PROPOSAL

Emma Aldibs¹, Tervel Bobev,² Louise De Béthune,³ Ella De Noyette,⁴ Laura Drechsler,⁵ Charlotte Ducuing,⁶ Abdullah Elbi,⁷ Irmak Erdogan,⁸ Ezgi Eren,⁹ Sara Garsia,¹⁰ Eyup Kun,¹¹ Javier Lopez-Guzman,¹² Julie Mannekens,¹³ Raminta Matulytė,¹⁴ Isabela Rosal Santos,¹⁵ Andrea Palumbo,¹⁶ Alexandra Papageorgiou,¹⁷ Bilgesu Sumer¹⁸

Introductory remarks

On 19 November 2025, the European Commission issued two proposals at the core of the current public consultation – the Digital Omnibus Proposal and the AI Omnibus Proposal. Both proposals include a number of ‘simplifying’ amendments of the current digital acquis ranging from data protection to cyber-security, to AI governance. The proposals touch upon many aspects that we are researching and analysing at the Centre for IT and IP Law (CiTiP), and we therefore want to contribute to its public discussion in this consultation, offering a perspective grounded in fundamental legal research. To this end, we took a researcher-led approach, whereby each contributing researcher or a group of researchers analysed and discussed the provisions of the proposals that matched their current research projects. Using this approach, we were able to offer a deep analysis of the provisions in question, which we found preferable to a comprehensive analysis, which this text does not provide. Our goal is to offer doctrinally grounded recommendations to the European Commission in order to improve the proposals and ensure they align with the legal principles of EU law, in particular the Charter of Fundamental Rights. While this contribution represents a large number of researchers at CiTiP it only represents the views of those who contributed.

Our contribution to the public consultation proceeds as follows: Part 1 discusses overarching concerns with both proposals and the approach taken therein. Part 2 discusses some of the changes proposed for the General Data Protection Regulation (GDPR) via the Digital Omnibus

¹ Corresponding author of Section 3.2.

² Corresponding author of Section 2.7.

³ Corresponding author of Sections 1.

⁴ Corresponding author of Section 4.1; 4.7.

⁵ Editor.

⁶ Corresponding author of Sections 1, 2.1, 2.2, 4.5.

⁷ Corresponding author of Sections 2.3, 2.4, 2.7, 3.2.

⁸ Corresponding author of Sections 1, 2.2; editor.

⁹ Corresponding author of Sections 2.1, 2.2, 2.3; assistant editor.

¹⁰ Corresponding author of Sections 2.7, 4.1, 4.3.

¹¹ Corresponding author of Sections 2.8, 4.6.

¹² Corresponding author of Section 1.

¹³ Corresponding author of Section 2.1, 2.5; assistant editor.

¹⁴ Corresponding author of Section 2.6.

¹⁵ Corresponding author of Section 4.2.

¹⁶ Corresponding author of Section 3.1.

¹⁷ Corresponding author of Sections 1, 4.4, 4.5; assistant editor.

¹⁸ Corresponding author of Sections 2.1, 2.4.

Proposal. Part 3 highlights changes proposed in the AI Omnibus Proposal to the AI Act. Part 4 returns to the Digital Omnibus Proposal and discusses changes that are not linked to the processing of personal data, namely changes to the Data Governance Act, the Data Act, and the EU's cybersecurity acquis. Each part is divided into sub-sections per proposed changes, which always conclude with a concrete recommendation for the European Commission for moving forward (except for Part I which includes general considerations).

Table of Contents

1. Overarching concerns with both proposals	4
1.1 Simplification v deregulation.....	4
1.2 Democratic deficit	4
2. Proposed changes to the General Data Protection Regulation (GDPR)	11
2.1 The definition of personal data	11
2.2 The definition of scientific research and the exception from the principle of purpose limitation	16
2.3 The new processing ground for special categories of personal data for AI training and development	21
2.4 The new processing ground for biometric data	21
2.5 Abuse of data subject rights	24
2.6 New exemptions for transparency	28
2.6.1 Article 13(4) of the GDPR	29
2.6.2 Article 13(5) of the GDPR	34
2.7 Automated decision-making and profiling	36
2.8 Cybersecurity and the GDPR (Art. 88a)	39
3. AI Omnibus Proposal	42
3.1 Governance architecture of the AI Act	42
3.2 AI Literacy	44
4. Other changes proposed in the Digital Omnibus Proposal	48
4.1 The new pro-industry approach towards data legislation	48
4.2 Implications of merging the Open Data Directive, the Data Governance Act into the Data Act	50
4.3 The unsolved issues with institutionalised data sharing	52
4.4 Access by public authorities to privately-held data on the basis of an exceptional need	54
4.5 Competent authorities and enforcement under the Data Act	56
4.6 Changes to the cybersecurity framework	57
4.7 Trade secrets	59
4.7.1 Trade secrets in the Data Act	60
4.7.2 Trade secrets in the Data Governance Act	62
References	64

1. Overarching concerns with both proposals

1.1 Simplification v deregulation

A deregulation on of the EU digital *acquis* comes at a time when the EU risks economic stagnation and pressures on digital competitiveness. Simplifying the regulatory framework may reduce administrative burdens, clarify obligations for businesses, and support innovation. At the same time, simplification should not overstep into deregulation. Deregulation only benefits the strongest players in the market and decreases fundamental rights protection and internal market business stability. As discussed in more detail below, some of the proposed changes in the Digital Omnibus amount to deregulation. Notable examples are the proposed changes in the definition of personal data under GDPR, and the moratorium on specific aspects of the AI Act. These changes are unlikely to significantly enhance the competitiveness of European companies in the digital market, as they introduce elements of legal and regulatory uncertainty. In this context, there is a risk that both market stability and the enforcement of citizens' rights end up being compromised.

Democratic regulation of data and technology can be done in multiple ways. Legislation is one way, mechanisms which allow for more flexibility, such as recommendations and even self-regulatory initiatives, such as standards, are another possible option. The current attempt at so-called simplification can best be compared to deregulation. Nevertheless, deregulation rarely has a positive impact on the fundamental rights of citizens; instead, it entails inconsistencies and legal uncertainty. Assimilating the data *acquis* into a one-size-fits-all data act may streamline legal obligations with business goals,¹⁹ yet does so at the cost of fundamental rights. This approach represents a potential departure from the Brussels effect, where the EU harnessed fundamental rights throughout market dynamics.²⁰ By loosening existing safeguards in pursuit of cost reduction and AI competitiveness, the Digital Omnibus risks weakening the regulatory leverage that previously reinforced these protections.²¹

The proposed optimisation of the digital rule book risks eroding the very foundations of these laws. Some predominant examples, which will be discussed in detail in the following parts of the opinion, are the revision to the definition of 'personal data', of the broadened definition of 'research' that shall now include – and therefore partially exonerate – innovation and of the addition of an irrefutable presumption that AI development finds a suitable legal basis for processing personal data. This is why many commentators identify, with the Digital Omnibus, a 'deregulatory' rather than a 'simplificatory' objective.

1.2 Democratic deficit

Omnibus legislation has become an increasingly common feature of EU law-making. This is particularly the case when the European Commission seeks to consolidate multiple measures into a single legislative act for the sake of efficiency or simplification. Only in 2025, the Commission proposed ten omnibus proposals.²² The Commission Work Programme 2026

¹⁹ European Commission (ed), 'The Future of European Competitiveness: Part A: A Competitiveness Strategy for Europe' (Publications Office 2025) <<https://doi.org/10.2872/9356120>>.

²⁰ Mario Draghi, 'The Future of European Competitiveness' (2024).

²¹ Felix Bieker and Katherine Nolan, 'European AI FOMO' [2026] Verfassungsblog <<https://doi.org/10.59704/8ea454b6677b517f>> accessed 5 March 2026. *ibid.*

²² European Commission, '2025 - Commission Proposals (Omnibus Packages)' <https://commission.europa.eu/document/download/9e358345-31e8-4cdd-8816-a30138ed07fe_en?filename=2025_%20Omnibus%20packages_List_for_Europa.pdf%3E>.

indicates ‘a new series of simplification initiatives and omnibus packages’ is to come.²³ In view of these recent initiatives, before examining the Digital Omnibus and AI Omnibus proposals, it is necessary to examine the meaning and implications of omnibus law-making, given its extensive use.

The omnibus negotiations pursue predominantly economic aims such as reducing compliance burdens and strengthening Europe’s competitive position. In that regard, the Simplification Agenda of the Commission invites the European Parliament and the Council to consider ‘fast-tracking these files,’ meaning the series of Omnibus packages and other simplification proposals, ‘to provide maximum and swift clarity and relief to companies’.²⁴

These legal instruments, by their nature, combine diverse and sometimes complex amendments that address ‘numerous and not necessarily related subjects, issues, and programs’.²⁵ This heterogeneity is highly relevant for the assessment that follows, as it affects the context in which the proposals must be evaluated. Moreover, omnibus legislations are typically enacted through an expedited legislative process that diverts from regular procedures.²⁶

The Commission justifies the Digital Omnibus proposal by referring to a few evidentiary considerations related to its stated objective. Most of these are self-assessments by the Commission, included in the accompanying Staff Working Documents. Staff Working documents present ‘estimated impacts’ asserting that the proposed simplifications will strengthen competitiveness, improve operational efficiency, reduce administrative burdens, and enhance legal certainty,²⁷ largely based on global privacy spending trends and some stakeholder perceptions.²⁸ However, in some parts, the Staff Working Document explicitly acknowledges that ‘it is not possible to support these claims with precise figures’.²⁹ It recognizes that, in terms of ex-post evaluations / fitness checks, most of the legislation under consideration in the Digital Omnibus proposal is not only recent but also subject to ongoing evaluation of results.³⁰

²³ European Commission, ‘Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions - Commission Work Programme 2026 - Europe’s Independence Moment’ COM(2025) 870 final, 21/10/2025 8.

²⁴ European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Simpler and Faster Europe*, COM(2025) 47 final, p. 6.

²⁵ Ittai Bar-Siman-Tov, ‘An Introduction to the Comparative and Multidisciplinary Study of Omnibus Legislation’ *Comparative Multidisciplinary Perspectives on Omnibus Legislation* (2021) 4.

²⁶ See also European Commission, ‘2025 - Commission Proposals (Omnibus Packages)’ (n 22).

²⁷ European Commission, ‘Commission Staff Working Document Accompanying the Documents - Proposal for a Regulation Amending Regulations (EU) 2016/1679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854, (EU) 2024/1689 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as Regards the Simplification of the Digital Legislative Framework, and Repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus) - Amending Regulations (EU) 2024/1689 and (EU) 2018/1139 as Regards the Simplification of the Implementation of Harmonised Rules on Artificial Intelligence (Digital Omnibus on AI)’ (2025) SWD(2025) 836 final.

²⁸ See for example for the proposals regarding the GDPR, *ibid* 34–35.

²⁹ *ibid* 34.

³⁰ European Commission, ‘Proposal for a Regulation Amending Regulations (EU) 2016/1679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854, (EU) 2024/1689 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as Regards the Simplification of the Digital Legislative Framework, and Repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus)’ (2025) COM(2025) 837 final 2025/0360 (COD) 11 <<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52025PC0837>>; For example, the Commission commissioned an evaluation study of the Data Governance Act, the Free-Flow of Non-Personal Data Regulation and of the Open Data Directive to

As to the expected impact of the Digital Omnibus Proposal, the Staff Document particularly concentrates on the SMEs and small operators, without accompanying a quantified distributional analysis or an assessment of cumulative effects on different categories of potential subjects which might be impacted. This approach is justified by the assumption that the amendments would not negatively affect fundamental rights and will preserve the same standards of protection.³¹ These assertions, however, appear to be self-referential, as they are presented without a dedicated fundamental rights impact assessment to substantiate them. Furthermore, the Staff Document builds largely on prior impact assessments³² conducted for the original instruments and provides projected cost savings. However, it does not reevaluate whether the omnibus amendments themselves alter the balance between ‘burden reduction’ and fundamental rights protection.

Prior to the recent reform packages, the EU had only sparingly resorted to omnibus legislative techniques, with isolated examples such as the consolidation of consumer protection law³³ and the streamlining of certain post-Lisbon procedural frameworks³⁴ that produced tangible administrative simplification. Nevertheless, the 2025 omnibus bills and those that follow mark a decisive shift in EU legislative practice: what was once an exceptional tool is now applied systematically, in terms of both number and scope. First, their routine use has normalised deviations from the EU’s traditional legislative order, turning exceptions to the regular lawmaking process into the norm. Second, the content of the omnibus bills has diverged sharply from the simplification-oriented approach envisaged under the Commission’s Better Regulation rules, as set out in Better Regulation ‘Guidelines’³⁵ and related ‘Toolbox’.³⁶ Since 2025, the omnibus packages have done more than just streamline administrative procedures. They have also altered the nature and purpose of obligations by raising legal thresholds, softening incumbent duties, deferring enforcement, and revoking established standards.³⁷

The EU Commission’s Better Regulation framework emphasises that legislation should be targeted, effective, easy to comply with, and impose the least possible burden.³⁸ Such a regulation is achieved through a structured, evidence-based approach *combining* several evaluations, fitness checks, impact assessments, and stakeholder consultation.³⁹

consultancy agencies. Even though these legislations are in the scope of the revision introduced by the Digital Omnibus Proposal, the Commission did not take into account the evaluation, the final report of which was published only a month after the issuance of the Digital Omnibus Proposal. Capgemini and others, ‘Study Supporting the Evaluation of the Free Flow of Non-Personal Data Regulation, Open Data Directive and Data Governance Act’ (European Commission 2025) <<https://data.europa.eu/doi/10.2759/8620781>> accessed 5 March 2026.

³¹ Ibid 4, 43.

³² Ibid 30, 46, 62, 69, 81.

³³ Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules (OJ L 328/7, 18/12/2019).

³⁴ Regulation (EU) 2019/1243 of the European Parliament and of the Council of 20 June 2019 adapting a number of legal acts providing for the use of the regulatory procedure with scrutiny to Articles 290 and 291 of the Treaty on the Functioning of the European Union (Text with EEA relevance) (OJ L 198/241, 20/6/2019).

³⁵ European Commission, ‘Better Regulation Guidelines’ (European Commission 2021) SWD(2021) 305 final.

³⁶ European Commission, ‘Better Regulation Toolbox’ (2023).

³⁷ Alberto Alemanno, ‘The Omnibus Road to Constitutional Drift: How the Rise of Omnibus Legislation Undermines Procedural Integrity in the EU’ (Verfassungsblog, 12 November 2025) <https://verfassungsblog.de/omnibus-legislation-europe-constitutional/> accessed 24.02.2026

³⁸ European Commission, ‘Better Regulation Guidelines’ (n 35) 3.

³⁹ Ibid.

Evaluations and fitness checks assess whether existing measures remain fit for purpose, identify inefficiencies and effectiveness.⁴⁰

Impact assessments systematically analyse problems, policy options, trade-offs, and potential impacts. They assess the environmental, social, and economic impacts of chosen policies.⁴¹ Crucially, impact assessments identify who will be affected by the proposed measures and in what way, and also enable an evaluation of impacts from the perspective of society.⁴² Based on evidence gathered from data, scientific advice, and stakeholder input, they seek to ensure that policy choices rely on objective analysis and remain transparent and accountable.⁴³ Consequently, they play a central role in demonstrating that a legal measure is suitable, necessary, and proportionate to the objectives pursued, thereby contributing to compliance with the principle of proportionality.

In this context, the absence of a proper impact assessment, the scarcity of evidentiary facts, the limited consultations and the accelerated procedure for the legislative adoption of the Digital Omnibus Proposal shall be legally appraised in light of the general principles of necessity, proportionality and of the principle of evidence-based policymaking established in the Better Regulation framework and in the Interinstitutional Agreement on Better Law-Making upon which the EU institutions, as law-makers, bound themselves to certain standards when making laws.⁴⁴

The general principle of proportionality, while fully applicable to the adoption of secondary legislation, does not prejudice the broad discretion that the EU policy- and lawmakers enjoy when making decisions involving political, economic and social dimensions. This broad discretion applies primarily to the nature and scope of the measures and, to some extent, to the finding of the basic facts underpinning them.⁴⁵ This implies that, in such scenarios, EU policy- and law-makers are not bound to adopt a particular type of measure in view of their alleged policy objective. As a result, the Better Regulation framework and the Interinstitutional Agreement recognise exceptions to the requirement to conduct an impact assessment in view of particular circumstances.⁴⁶ Yet, the discretion of the EU law-maker is limited by the requirement that they do not adopt a measure that is manifestly inappropriate in view of the objective.⁴⁷ Besides, their broad discretion is also a responsibility that they shall demonstrably exercise while making laws, resulting in enhanced transparency requirements as to the facts deemed relevant for making policy and legislative decisions. Such facts shall include available scientific facts and other available.⁴⁸ Failing that, the EU lawmaker would act in breach of the general principle of proportionality.

⁴⁰ *ibid* 9, 10.

⁴¹ *ibid* 10.

⁴² *ibid* 35.

⁴³ *ibid* 34, 35.

⁴⁴ Interinstitutional Agreement between the European Parliament, the Council of the European Union and the European Commission on Better Law-Making (OJ L 123/1, 12/5/2016).

⁴⁵ *Republic of Poland v European Parliament and Council of the European Union* [2018] ECI Case C-5/16 125.

⁴⁶ *ibid* 83.

⁴⁷ *The Queen, on the application of Vodafone Ltd and Others v Secretary of State for Business, Enterprise and Regulatory Reform* [2010] ECI Case C-58/08 para 52.

⁴⁸ *Republic of Poland v European Parliament and Council of the European Union* (n 45) para 152-153; 160-163.

In view of that, the alleged ‘urgency’⁴⁹ of the adoption of the Digital Omnibus Proposal as a ‘particular circumstance’ shall, first, be challenged, as the Commission does not demonstrate any such concrete urgency⁵⁰ but merely refers abstractly to the need for innovation-friendly rules in order to ensure the competitiveness of European industry on the international plane. Moreover, the Digital Omnibus Proposal proposes to revise rules that, for some of them, are not even yet in force and have therefore not produced any direct legal effect at the time of the adoption of the Digital Omnibus Proposal. Besides, the adoption of some of these rules – such as Data Act – were precisely and overwhelmingly justified by innovation.⁵¹ These elements call into question the argument that the Digital Omnibus Proposal justifies departing from standard impact assessments and detailed justifications on the basis of an urgent need to promote innovation. In particular, relying on innovation to limit evidentiary analysis appears paradoxical given that the innovation-friendliness of laws has, until this point, been consistently associated with science- and fact-based law-making, including by the Commission.⁵²

The second issue pertains to the objective allegedly pursued by the Commission, namely ‘simplification’ of the rules. According to the Commission, this objective justifies a fast-tracked legislative procedure without a proper impact assessment as the proposal would not result in any significant implications for the protection of fundamental rights. Nevertheless, as discussed by many commentators and throughout this contribution, many proposed revisions do have a significant - i.e. *detrimental* - impact on the protection of fundamental rights, as they generally tend to lower protection, especially with respect to the GDPR.⁵³ And yet, the Commission does not pursue a fundamental rights impact assessment and, in particular, does not assess the impact of the proposed measures on the right to data protection of individuals.⁵⁴ The only fundamental right on which the Commission analyses the impact of the Digital Omnibus Proposal is the freedom to conduct a business. The Commission considers that the legislative support of the Digital Omnibus Proposal to innovation opportunities for

⁴⁹ European Commission, ‘Digital Omnibus’ (n 29) recital 60.

⁵⁰ A similar critique was raised by the European Ombudsman to the European Commission concerning the adoption of several legislative proposals; see European Ombudsman, ‘Recommendation on the European Commission’s Compliance with “Better Regulation” Rules and Other Procedural Requirements in Preparing Legislative Proposals That It Considered to Be Urgent (983/2025/MAS - the “Omnibus” Case, 2031/2024/VB - the “Migration” Case, and 1379/2024/MIK - the “CAP” Case)’. This notably concerns another ‘omnibus’ legislative proposal in the similar context where the ‘simplification’ or weakening of rules was deemed to be urgently needed for innovation and international competitiveness; see European Commission, ‘Proposal for a Directive of the European Parliament and of the Council Amending Directives 2006/43/EC, 2013/34/EU, (EU) 2022/2464 and (EU) 2024/1760 as Regards Certain Corporate Sustainability Reporting and Due Diligence Requirements’ (2025) COM(2025) 81 final-2025/0045 (COD).

⁵¹ The Data Act project to require data sharing in various scenarios is heavily grounded in the goal to steer innovation, competitiveness and economic growth, see in particular recital 1 of the Data Act (Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act) (Text with EEA relevance) [OJ L 2023/2854, 13/12/2023]). This is particularly the case for the regulation of connected product data in Chapter II (see, inter alia, recitals 15, 20 and 32).

⁵² See for example European Commission, ‘Ensuring EU Legislation Supports Innovation: The Innovation Principle as a Research and Innovation Tool for Innovation Friendly Regulation’ <https://research-and-innovation.ec.europa.eu/law-and-regulations/ensuring-eu-legislation-supports-innovation_en> accessed 5 March 2026. For a synthesis, see Charlotte Ducuing, ‘A Legal Principle of Innovation? Need for an Assessment Against the Principle of Democracy’ (2022) 14 Law, Innovation and Technology 237 <<https://doi.org/10.1080/17579961.2022.2113667>>.

⁵³ European Commission, ‘Proposal for a Regulation Amending Regulations (EU) 2016/1679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854, (EU) 2024/1689 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as Regards the Simplification of the Digital Legislative Framework, and Repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus)’ (2025) COM(2025) 837 final 2025/0360 (COD) 15.

⁵⁴ *ibid.*

businesses promotes this ‘right’ (sic).⁵⁵ However, this approach risks treating ‘innovation’ as if it were a Treaty-protected right, effectively turning it into a subjective right of companies enforceable against lawmakers.

Besides, areas in notorious need of simplification have been left entirely untouched by the Digital Omnibus Proposal. For example, the lack of consistency between the concepts used across the various legislative frameworks at hand⁵⁶ raises feasibility and effectiveness issues. While not a simplification measure in itself, the Digital Omnibus Proposal was a – thus missed opportunity for an overall clarification and streamlining of the concepts and for a clarification of the potential overlaps between legislations. Another missed opportunity for simplification concerns the complex public enforcement mechanisms that EU data legislations – such as the Data Governance Act (DGA)⁵⁷ and the Data Act⁵⁸ – have established. They require member States to set up complicated and costly cooperation mechanisms among a large array of public enforcers within and across borders, potentially delaying or even impeding – rather than facilitating – enforcement. Some commentators have proposed regulating and harmonising cooperation at the EU level.⁵⁹ The scope of regulatory supervision and enforcement could – alternatively or complementarily – be reduced.⁶⁰ In any case, EU legislative revision would be required for such a simplification endeavour.⁶¹ Here again, the Commission Digital Omnibus Proposal comes across as a missed opportunity for (i.e. genuine) simplification. These developments signal inconsistencies between the alleged objective of the Digital Omnibus Proposal and the actual measures that it puts forward. They expose the unfoundedness of the simplification objective, thus restoring the requirement for conducting a proper impact assessment.

Third, procedurally and related to the above, the reliance on targeted ‘Reality Checks’ with only selected industry actors, instead of broad and inclusive public consultations, raises concerns regarding participation, openness, and sufficient time for stakeholder engagement.⁶² Instead of 12-week public consultations, the Commission used targeted events, calls for

⁵⁵ *ibid.*

⁵⁶ Charlotte Ducuing, *Data Commodification and the Law: Navigating Data Markets and Data Protection* (Intersentia 2025); Inge Graef and Bart Van Der Sloot (eds), *The Legal Consistency of Technology Regulation in Europe* (1st edn, Hart Publishing 2024) <<https://doi.org/10.5040/9781509968053>>; Julie Baloup and others, ‘White Paper on the Data Governance Act’ (2021) Section 3.2 onwards.

⁵⁷ Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (Text with EEA relevance) (OJ L 152/1, 30/5/2022).

⁵⁸ Data Act.

⁵⁹ Paul De Hert and Paweł Hajduk, ‘EU Cross-Regime Enforcement, Redundancy and Interdependence: Addressing Overlap of Enforcement Structures in the Digital Sphere After Meta.’ (2024) 2024 *Technology and Regulation* 291 <<https://doi.org/10.71265/fydws959>>; Charlotte Ducuing and Alexandra Papageorgiou, ‘Commentary of Article 37 Data Act’ *EU Data Law: A Commentary on the DGA and the DA* (Elgar 2026).

⁶⁰ Josef Drexel and others, ‘Position Statement of the Max Planck Institute for Innovation and Competition of 25 May 2022 on the Commission’s Proposal of 23 February 2022 for a Regulation on Harmonised Rules on Fair Access to and Use of Data (Data Act)’ (Max Planck Institute for Innovation and Competition 2022) 86–88 <https://www.ip.mpg.de/fileadmin/ipmpg/content/stellungnahmen/Position_Statement_MPI_Data_Act_Formal__13.06.2022.pdf> accessed 5 March 2026; Charlotte Ducuing, Thomas Margoni and Luca Schirru (eds), ‘White Paper on the Data Act Proposal’ (2022) s 13 (Chapter IX-Data-specific enforcement, Charlotte Ducuing and Aliko Benmayor) <<https://www.law.kuleuven.be/citip/en/Publications/citip-whitepaperdataact.pdf>> accessed 5 March 2026.

⁶¹ This does not take away the relevance of soft law initiatives, such as, predominantly, the Digital Clearinghouse 2.0 concept proposed by the EDPS, see European Data Protection Supervisor (EDPS), ‘Towards A Digital Clearinghouse 2.0’ (2025) <https://www.edps.europa.eu/system/files/2025-01/towards_a_digital_clearinghouse_2_0_january_2025_en_0.pdf> accessed 21 February 2025.

⁶² For the importance of these principles, see European Commission, ‘Better Regulation Guidelines’ (n 35) 14–17.

evidence, and bilateral meetings. In that regard, stakeholder mapping focused on the actors who will implement the rules, thus sidelining other *actors that these policies will affect*.⁶³

In conclusion, the Digital Omnibus Package raises serious issues regarding compliance with both the Better Regulation framework and the general principle of proportionality outlined in Article 5(4) of the Treaty on European Union that seek to ensure the democratic accountability of EU secondary legislation. Democratic issues are particularly striking when it comes to the invocation of ‘urgency’, ‘innovation’ and (mere) ‘simplification’ as alleged justifications for doing away with democratic procedures, transparency and fact-gathering requirements. These findings should be read in the broader context of the Commission's extensive recourse to omnibus procedures, paving the way for a deregulatory agenda without the necessary democratic safeguards. Finally, while the Digital Omnibus Package is based on both an urgency rationale and an (alleged) simplification objective, the two are not necessarily compatible. As further developed in the remainder of this contribution, there are several unclarities and misalignments in the Omnibus, especially following the merger of several data-related legislative frameworks. A result of the ‘urgency’ or hastiness, these issues run directly against the simplification objective of the Commission.

⁶³ In contrast to Better Regulation Guidelines, *ibid* 17. The same critique was raised by the European Ombudsman concerning the adoption of several legislative proposals including an omnibus; see European Ombudsman (n 50). The Ombudsman observed a similar selection of the consulted stakeholders and interrogated the Commission as to the rationale for such an imbalanced representation, which the Commission was unable to justify.

2. Proposed changes to the General Data Protection Regulation (GDPR)

2.1 The definition of personal data

The Digital Omnibus Proposal fundamentally changes the definition of personal data in Article 4(1) General Data Protection Regulation (GDPR).⁶⁴ The definition of ‘personal data’ is of vital importance since it is decisive on whether the GDPR applies. Data protection law primarily centres on personal data to safeguard the privacy and related interests of individuals, which are protected as fundamental rights and freedoms. Respect for private and family life and the protection of personal data is enshrined in Articles 7 and 8 of the EU Charter of Fundamental Rights, as well as in Article 8 of the European Convention on Human Rights.⁶⁵ In light of this fundamental rights framework, European data protection law, including the GDPR, has consistently adopted a broad concept of personal data in order to ensure a high level of data protection.⁶⁶ From the beginning, this has also been a deliberative choice of the European legislator grounded in the recognition of the protection of personal data as a fundamental right.⁶⁷

Despite the GDPR’s apparent affinity with an absolute approach to personal data, the Court of Justice (‘CJEU’) has favoured a relative approach, nuanced by the requirement that data qualify as personal where the data subject is identifiable by the controller or any other person, as articulated in recital 26 GDPR.⁶⁸ Nevertheless, the evolution of the concept in the CJEU’s case law⁶⁹ aligns with a broader interpretative approach. We contend in this section that the proposal risks the EU abandoning its broad conception of personal data in favour of a strictly relative interpretation. We argue that the proposal introduces several significant problems that could undermine the data protection - and, in general, fundamental rights - framework. We identified four main issues related to the proposed changes: (i) the Digital Omnibus Proposal contradicts the case law of the CJEU; (ii) changing the definition of personal data in the GDPR risks destabilising the whole EU digital law framework; (iii) over-technicalisation in data protection law neglects the objectives of the GDPR; (iv) delegating the task of determining the identifiability in specific contexts risks leading to institutional imbalances (and power imbalances in general) in a highly normative context that regards fundamental rights and freedoms.

⁶⁴ European Commission, ‘Digital Omnibus’ (n 30) 54–55.

⁶⁵ Charter of Fundamental Rights of the European Union 2000 (2000/C 364/01); Convention for the Protection of Human Rights and Fundamental Freedoms 1950.

⁶⁶ Article 4(1) of the GDPR defines personal data as any information relating to an identified or identifiable natural person (data subject). Recital 26 of the GDPR states: “To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly.” Recital 30 of the GDPR states that: Natural persons may be associated with online identifiers provided by their devices, applications, tools, and protocols, such as internet protocol addresses, cookie identifiers, or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.

⁶⁷ European Commission, ‘Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions A Comprehensive Approach on Personal Data Protection in the European Union’ COM(2010) 609 final, 4/11/2020 5 <<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52010DC0609>> accessed 5 March 2026.

⁶⁸ Also see *Patrick Breyer v Bundesrepublik Deutschland* [2016] ECJ Case C-582/14.

⁶⁹ See cases: *ibid*; *Gesamtverband Autoteile-Handel eV v Scania CV AB* [2023] ECJ Case C-319/22; *OC v European Commission* [2024] ECJ Case C-479/22 P ECLI:EU:C:2024:215; *IAB Europe v Gegevensbeschermingsautoriteit* [2024] ECJ Case C-604/22.

Problem 1: The Digital Omnibus Proposal has generalised *EDPS v. SRB*, without taking into account the specific circumstances of this case. Moreover, the definition in the Digital Omnibus Proposal goes beyond and even contradicts established case law of the CJEU.

As the EDPS and EDPB emphasized in their Joint Opinion, the GDPR, including the definition of personal data, must be interpreted in light of the whole body of CJEU jurisprudence.⁷⁰

In *EDPS v. SRB*, the CJEU considered that depending on the circumstances, pseudonymisation may effectively prevent persons other than the controller from identifying the data subject in such a way that, for them, the data subject is not or is no longer identifiable.⁷¹ The Commission seems to rely on this reasoning in proposing that '*information shall not be personal for a given entity where that entity cannot identify the natural person to whom the information relates, taking into account the means reasonably likely to be used by that entity*'. Indeed, both the Working Staff Document⁷² and recital 35 of the Digital Omnibus Proposal state that, taking into account the case law of the CJEU, information is not to be considered personal data for a given entity where that entity does not have the means reasonably likely to be used to identify the natural person. However, it is notable that the CJEU used the wording 'may' several times, while the definition in the Digital Omnibus Proposal uses the notion 'shall'.⁷³ Using the wording 'may' emphasises that the specific circumstances of each case should be taken into account. In this regard, the CJEU considered two specific points in *EDPS v. SRB*: (i) the recipient must have no possibility of reversing the pseudonymisation, and (ii) the measures taken must preclude the pseudonymised data from being linked to an individual, for example, through comparison with other (external) data sources.⁷⁴ By using 'shall' rather than 'may', the definition risks overriding the specific circumstances of each case.

Moreover, the Digital Omnibus Proposal contradicts the CJEU's reasoning in the case *Gesamtverband Autoteile-Handel eV Scania CV A*.⁷⁵ In *EDPS v. SRB*, the CJEU referred to the *Scania* judgement and observed that the transfer of data, that are in themselves 'impersonal' may render such data 'personal' where the controller puts them at the disposal of other persons who have the means reasonably likely to enable the data subject to be identified.⁷⁶ The *Scania* judgement concerned the transfer of the vehicle identification number (VIN number) by vehicle manufacturers to independent operators. The manufacturer itself does not have the means to link the VIN number to an individual, while the independent operators have. The CJEU ruled that since the independent operators can link the VIN number to an identified or identifiable natural person, the VIN number constitutes personal data for them, and indirectly for the manufacturers making it available.⁷⁷ On the basis of this judgement, it could be argued that the GDPR applies to the manufacturer transferring the VIN number, and; therefore, the manufacturer should take into account the obligations arising from the GDPR. The Digital Omnibus Proposal now explicitly excludes the applicability of the GDPR for the

⁷⁰ European Data Protection Board (EDPB) and European Data Protection Supervisor (EDPS), 'Joint Opinion 2/2026 on the Proposal for a Regulation as Regards the Simplification of the Digital Legislative Framework (Digital Omnibus)' (2026) para 15.

⁷¹ *European Data Protection Supervisor v Single Resolution Board* [2025] ECJ Case C-413/23 P ECLI:EU:C:2025:645 para 86.

⁷² European Commission, 'SWF Digital Omnibus' (n 27) 38.

⁷³ *European Data Protection Supervisor v Single Resolution Board* (n 71) paras 75,77 and 86.

⁷⁴ *ibid* para 77.

⁷⁵ *Gesamtverband Autoteile-Handel eV v Scania CV AB* (n 69).

⁷⁶ *European Data Protection Supervisor v Single Resolution Board* (n 71) para 84.

⁷⁷ *Gesamtverband Autoteile-Handel eV v Scania CV AB* (n 69) para 49.

manufacturer in such context by indicating that ‘*such information does not become personal for that entity merely because a potential subsequent recipient has means reasonably likely to be used to identify the natural person to whom the information relates*’. Therefore, the Digital Omnibus Proposal contradicts the CJEU reasoning in the *Scania* judgement. In this regard, the EDPB and EDPS have also highlighted in their Joint Opinion that this last sentence of the definition of personal data in the Digital Omnibus Proposal does not accurately reflect and clearly goes beyond the CJEU jurisprudence.⁷⁸

Lastly, it should be recalled that when interpreting and applying law, context remains crucial. As the EDPB and EDPS highlighted in their Joint Opinion, a selective codification of case law of the CJEU by introducing only a single element from a single case, lacks the necessary context.⁷⁹ In *EDPS v. SRB*, the CJEU has reaffirmed that the relevant perspective for assessing whether a natural person is identifiable depends on the circumstances of each individual case.⁸⁰ Accordingly, drawing broad conclusions from a single case is unlikely to provide a reliable basis for the way forward.

Different perspectives have already been taken into account in previous case law of the CJEU. In *EDPS v. SRB*, the CJEU considered that, depending on the circumstances, a recipient of pseudonymised data may indeed be effectively prevented from identifying an individual. As a result, the CJEU assessed the situation from the perspective of the recipient.⁸¹ Recalling *OC v. Commission*, the CJEU held that although the data subject was not named in the published press release, it nevertheless contained information enabling identification, in particular by those working in the same scientific field and familiar with that person’s professional background.⁸² Therefore, the CJEU took into account the perspective of the public concerned, namely all potential recipients, to conclude whether the transfer of pseudonymized data constituted a transfer of personal data. In *Scania*, the CJEU held that since the recipient can link the data to an identified or identifiable natural person, the data constitutes personal data for them, and indirectly for the transferors making it available.⁸³ As a result, the perspective of the recipient had an influence on the perspective of the transferor.⁸⁴

Before concluding this argument, it is important to remind that the current wording under the GDPR allows for the nuanced interpretation of personal data and identifiability, as demonstrated by the case law mentioned above. Recital 26 of the GDPR already provides a clear and strong enough basis for the contextual interpretation highlighted in the CJEU’s case law, without necessitating a change in the definition of personal data.

⁷⁸ European Data Protection Board (EDPB) and European Data Protection Supervisor (EDPS), ‘Joint Opinion 2/2026 on the Proposal for a Regulation as Regards the Simplification of the Digital Legislative Framework (Digital Omnibus)’ (2026).

⁷⁹ ‘EDPD-EDPS Joint Opinion 2/2026 On the Proposal for a Regulation as Regards the Simplification of the Digital Legislative Framework (Digital Omnibus)’ para 15 <https://www.edpb.europa.eu/system/files/2026-02/edpb_edps_jointopinion_202602_digitalomnibus_en.pdf> accessed 2 March 2026. European Data Protection Board (EDPB) and European Data Protection Supervisor (EDPS), ‘Joint Opinion 2/2026 on the Proposal for a Regulation as Regards the Simplification of the Digital Legislative Framework (Digital Omnibus)’ (n 78).

⁸⁰ *European Data Protection Supervisor v Single Resolution Board* (n 71) para 100.

⁸¹ *ibid* paras 77 and 87.

⁸² *OC v European Commission* (n 69) paras 60-63.

⁸³ *Gesamtverband Autoteile-Handel eV v Scania CV AB* (n 69) para 49.

⁸⁴ *Gesamtverband Autoteile-Handel eV v Scania CV AB* (n 69).

Problem 2: The GDPR serves as the central regulatory reference point within the EU digital laws, which repeatedly defers to the GDPR definition of personal data. A drastic alteration of this core concept risks destabilising the coherence of the digital regulatory framework.

Far from a self-contained legislation, the GDPR's definition of personal data is one of the core definitions of the EU digital sphere; it is expressly relied upon by a wide range of sector-specific legislation, including the AI Act, the Data Act, the Digital Services Act, eIDAS 2.0 and the Payment Services Directive, to name a few. These instruments consistently refer to the GDPR for determining when data qualify as personal and for delineating the applicable obligations. Consequently, the GDPR's definition of personal data functions not merely alongside these regimes, but as the normative anchor point that ensures conceptual coherence across the digital law space.

In this regard, this far-reaching revision proposal of the GDPR foundational concepts risks implications that extend beyond data protection law. Weakening or reconfiguring the scope of personal data would destabilise the foundations of the entire interconnected regulatory framework, potentially causing a ripple effect across the whole system. This not only threatens the internal consistency of the digital governance in the EU but also risks eroding legal certainty rather than enhancing it. In this sense, as rightly put by Purtova, "Logically, a restriction of the meaning of identifiability and hence of the concept of personal data will have a domino effect across all these domains, leading to the overall reduction of legal protection".⁸⁵ As a result, simplification might not be achieved; instead, the changes might lead to legal fragmentation, increased uncertainty over compliance, and reduced protection of fundamental rights. Moreover, while the Digital Omnibus Proposal proposes changes to the definition of personal data in the GDPR and the EUDPR,⁸⁶ it leaves the definition of personal data under the Law Enforcement Directive (LED)⁸⁷ untouched. This risks fragmentation of the EU data protection acquis.

Problem 3: The Commission's approach seems to shift the focus away from mitigating risks to fundamental rights, which has been one of the main objectives of the GDPR.

It should be noted that data protection law is already highly technical and over-technicalisation becomes increasingly prevalent, particularly with regard to concepts such as anonymisation and pseudonymisation. The Commission's proposed approach risks further shifting the regulatory focus away from the mitigation of these risks to fundamental rights towards an overly narrow and technically framed threshold of identifiability. We do not deny that the risk of identification is a relevant parameter, nonetheless, the scope of fundamental rights risks addressed by the GDPR is considerably broader and cannot be reduced to

⁸⁵ Nadya Purtova, 'Why Simply Redefining Personal Data Narrowly Does Not Solve the Problem of the "Law of Everything"' (*Brussels Privacy Hub*, 15 December 2025) <<https://brusselsprivacyhub.com/why-simply-redefining-personal-data-narrowly-does-not-solve-the-problem-of-the-law-of-everything/>> accessed 2 March 2026.

⁸⁶ Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (Text with EEA relevance.) (OJ L 295/39, 23/10/2018).

⁸⁷ Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA 2016 (OJ L).

questions of identifiability alone.⁸⁸ The GDPR is not about protecting personal data for its own sake but about protecting the natural persons and their fundamental rights behind the data.

Framing personal data solely around technical thresholds of identification risks obscuring accountability concerns and might even contribute to the emergence of responsibility gaps, particularly within complex data ecosystems, e.g., data spaces or blockchain-based personal data processing ecosystems. For instance, even where the risks of identification are deemed low from a technical perspective, data subjects may not find a correspondent, i.e., an accountable entity, to invoke their respective rights.

Problem 4: The Commission, together with the European Data Protection Board ('EDPB'), is tasked with developing technical criteria and implementing acts to specify state-of-the-art techniques and categories for assessing the risks of re-identification.⁸⁹ However, defining the limits of personal data based on technical criteria unilaterally determined by the Commission for pseudonymised data raises concerns regarding the institutional balance, independence and objectivity of the resulting standards.

The mandate given to the Commission to develop technical criteria and implementing acts defining the state-of-the-art pseudonymisation techniques and categories for assessing re-identification carries important governance implications. While these measures may contribute to harmonisation and provide practical clarity for stakeholders, they raise significant concerns for institutional balance and independence as they would involve core policy choices that should be reserved for legislative acts. In light of Article 291 TFEU on implementing acts, and consistent with CJEU case law on the division of institutional powers, the Commission's role in developing standards should not cross into law-making. This is specifically relevant for the identifiability threshold, which has substantial normative effects on the notion of personal data, and consequently, on fundamental rights and freedoms.⁹⁰ As highlighted by the EDPS and EDPB in their Joint Opinion, the definition of personal data has a direct effect on the material scope of EU data protection.⁹¹ In other words, the Commission should not act *ultra vires*, particularly on matters regarding fundamental rights and freedoms.

Moreover, the development of highly technical standards with normative effects through executive procedures can be particularly vulnerable to stakeholder influence, such as lobbying. Furthermore, stakeholders are not on an equal footing, since technical expertise and resources are often concentrated among certain industry actors, giving them a disproportionate ability to shape standards compared with others. The resulting criteria and acts might be influenced by dominant market interests, which can further prioritise economic considerations over fundamental rights. This type of procedure can also be difficult to contest, as it would only be partially transparent.⁹²

⁸⁸ The scope of risks in the GDPR covers more than the risks to the right to the protection of personal data. Katerina Demetrou, 'GDPR and the Concept of Risk: The Role of Risk, the Scope of Risk and the Technology Involved' in Eleni Kosta and others (eds), *Privacy and Identity Management. Fairness, Accountability, and Transparency in the Age of Big Data*, vol 547 (Springer International Publishing 2019) <https://doi.org/10.1007/978-3-030-16744-8_10> accessed 2 March 2026.

⁸⁹ European Commission, 'Digital Omnibus' (n 29) Arts 14a and recital 27.

⁹⁰ *European Parliament v Council of the European Union* [2012] ECI Case C-355/10, ECLI:EU:C:2012:516.

⁹¹ European Data Protection Board (EDPB) and European Data Protection Supervisor (EDPS), 'Joint Opinion 2/2026 on the Proposal for a Regulation as Regards the Simplification of the Digital Legislative Framework (Digital Omnibus)' (n 78) para 23.

⁹² On institutional balance, also see Meroni doctrine for unlawful delegation of discretionary power in private agencies. *Meroni & Co, Industrie Metallurgiche, SpA v High Authority of the European Coal and Steel Community* [1958] ECI Case 9-56, ECLI:EU:C:1958:7.

Recommendations

We recommend that any proposed changes to the core concepts of data protection law, such as personal data, shall be evidence-based and tested in advance for different scenarios and technological contexts to ensure that they do not produce undesirable consequences for the protection of fundamental rights and freedoms.⁹³

We believe it is preferable to maintain the existing definition of personal data. First, it should be recalled that the Convention 108 applies to personal data which is defined in Article 2(a) as *'any information relating to an identified or identifiable individual'*.⁹⁴ Taking into account the further clarifications in the Explanatory Report of Convention 108, which indicate that the definition in the Convention has essentially the same meaning as the current definition in the GDPR,⁹⁵ the level of protection afforded by the GDPR may in no event fall below that guaranteed by the Convention 108. Second, previous case law, in particular the CJEU's reasoning in *EDPS v. SRB*, demonstrates that the current definition of personal data allows for taking into account the specific circumstances of the case and for verifying whether a specific entity indeed has the means reasonably likely to be used to identify a data subject. Accordingly, there is no need to change the definition on the basis of a single case in which the specific factual circumstances play a decisive role, particularly where doing so would effectively contradict previous case law. Changing the definition to such an extent would open up the door to abuse, enabling controllers to argue that the GDPR does not apply. A more appropriate approach would be to entrust further clarification to the evolving case law of the CJEU and decisional practice of data protection authorities.

Lastly, core determinations on re-identification risks have normative effects that directly affect fundamental rights. These should not be defined through executive and technocratic processes, which risk lowering the level of fundamental rights protection across the digital regulatory framework. Our recommendation in that regard is that the political choices and matters affecting fundamental rights should be decided by the primary legislature rather than through executive procedures. Regarding the proposed mandate given to the Commission to develop technical criteria and implementing acts defining the state-of-the-art pseudonymisation techniques and categories for assessing re-identification risks, we believe that this provision should be removed. Instead, as also highlighted by the EDPB and EDPS in their Joint Opinion, it should be the competence of supervisory authorities, under the control of the competent courts, to independently apply the definitions of the GDPR. Furthermore, it is the competence of the EDPB to ensure consistent application on this matter.⁹⁶

2.2 The definition of scientific research and the exception from the principle of purpose limitation

The Digital Omnibus Proposal (Art. 3(1)(b)(38)) introduces a new definition of 'scientific research' to the GDPR, for the purpose of applying derogatory data protection rules, i.e. overall less stringent ones, thus balancing the right to data protection with the freedom of

⁹³ This is also required by the EU Better Regulation Principles. Felicitas Bitzenhofer, 'Better Regulation Guidelines | Interoperable Europe Portal' (28 July 2024) <<https://interoperable-europe.ec.europa.eu/collection/assessments/document/better-regulation-guidelines>> accessed 5 March 2026.

⁹⁴ Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981, ETS 108 1981.

⁹⁵ Council of Europe, 'Explanatory Report to the Protocol Amending the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data' (2018) Council of Europe Treaty Series-No. 223 17–20.

⁹⁶ European Data Protection Board (EDPB) and European Data Protection Supervisor (EDPS), 'Joint Opinion 2/2026 on the Proposal for a Regulation as Regards the Simplification of the Digital Legislative Framework (Digital Omnibus)' (n 78).

science. The Proposal defines scientific research as ‘any research which can also support innovation, such as technological development and demonstration. These actions shall contribute to existing scientific knowledge or apply existing knowledge in novel ways, be carried out with the aim of contributing to the growth of society’s general and wellbeing and adhere to ethical standards in the relevant research area. This does not exclude that the research may also aim to further a commercial interest’.

Problem 1: The proposal deepens the lack of clarity in the conditions of scientific research.

The Commission justifies this amendment in the **Staff Working Document (SWD (2025) 836 final)** as addressing an alleged ‘lack of clarity’ concerning the conditions of scientific research and facilitating innovation and competitiveness.⁹⁷ The proposal leaves, nevertheless, the core notion of ‘research’ still undefined and broad. The addition that ‘any research’ that ‘can also’ support innovation is covered expands the scope to mere possibilities with potential outcomes as ‘by-products’.⁹⁸

This definition confuses scientific research with innovation and is not grounded on a sound and well-accepted notion of scientific research. As a result, it risks over-broadening the scope of the derogatory rules designed for science to pure commercial activities, thus abusing and denaturing this derogation for purposes other than the furthering of science.

The freedom of scientific research is protected at the level of international law⁹⁹ and is a fundamental EU freedom enshrined in the EU Charter of Fundamental rights.¹⁰⁰ The 2017 UNESCO Recommendation on Science and Scientific Researchers defines ‘science’ as the enterprise whereby humankind makes an organized attempt, by means of a certain (i.e. scientific) methodology, to discover and master the chain of causalities, relations or interactions; brings together knowledge in a systematic reflection and conceptualization and thereby furnishes itself with the opportunity of using, to its own advantage, understand of the processes and phenomena occurring in nature and society’. Furthermore, ‘scientific research’ is defined as processes of scientific knowledge generation. As part of the definition of ‘research and development’, scientific research is thereby contrasted to ‘experimental development’. As for itself, experimental development is defined as the processes of adaptation, testing and refinement which lead to the point of practical applicability including as innovation.¹⁰¹ In other words, scientific research and innovation (i.e. potentially as part of ‘experimental development’) shall be distinguished from one another while the former may indeed feed the latter. In the EU, the freedom of scientific research is viewed as a pillar of democracy and as an indispensable prerequisite for our ‘social, cultural, political and

⁹⁷ European Commission, ‘SWF Digital Omnibus’ (n 27) 39.

⁹⁸ NOYB, ‘Digital Omnibus: First Analysis of Select GDPR and ePrivacy Proposals by the European Commission (Version 3.0)’ (2026) <<https://noyb.eu/sites/default/files/2025-12/noyb%20Digital%20Omnibus%20Report%20V1.pdf>> accessed 5 March 2026.

⁹⁹ See in particular Universal Declaration of Human Rights (adopted 10 December 1948) 217 A (III) art 27; and International Covenant on Economic, Social and Cultural Rights (adopted 16 December 1966, entered into force 3 January 1976) 993 UNTS 3 art 15.

¹⁰⁰ Charter of Fundamental Rights of the European Union art 13; See also Consolidated version of the Treaty on the Functioning of the European Union [2012] OJ C326/47 art 179.

¹⁰¹ UNESCO, ‘Recommendation on Science and Scientific Researchers’ (13 November 2017) SHS/BIO/PI/2017/3 Rev, art I.1.(a)(i) and (c).

economic resilience and progress' through the advancement of knowledge.¹⁰² In other words, innovation is just one possible positive outcome of scientific research and it can also be generated by other means.

In this context, the proposed definition of scientific research is misaligned with the commonly accepted notion of science and scientific research, due to the (unclear) connection that the Digital Omnibus Proposal makes to innovation.

On the one hand, the proposal could be read as defining scientific research *only* as such research that delivers on innovation ('any research which can also support innovation'), thus seemingly narrowing down its scope. This interpretation links research to innovation, which would mean that non-technological academic and fundamental research may paradoxically fall outside the definition. On the other hand, it could be read as *conflating* scientific research and innovation, referencing both aims of 'contribut[ing] to existing knowledge' (the typical primary purpose of science) *or* 'apply[ing] existing knowledge in novel ways' (the typical primary outcome of innovation). This interpretation is reinforced by the reference to the furthering of commercial interests (i.e. through innovation). Such conflation between scientific research and innovation may lead to an over-broadening of the scope of scientific research to innovation and to encompassing profit-driven processing activities easily as scientific research.

Additional issues may arise in this context. First, an internally inconsistent definition might lead to challenges in interpretation and possible (national) fragmentation— the very issues that an EU-wide harmonised definition should, in principle, eliminate. Second, the derogatory regime designed for scientific research is justified by the freedom of science and should therefore have the same scope. Otherwise, it would operate as a function creep, trumping the fundamental right to data protection under the guise of science while actually advancing *other objectives*, i.e. the furtherance of innovation. This could be to the detriment of genuine scientific research, which might be excluded from the regime if it does not lead to innovation. n. Such a development could also constitute a harmful reference and precedent for other (data-related) legislations that also design derogatory rules for science.

Problem 2: The proposed amendment destabilises the Overall Scientific Research Regime in the GDPR

The Staff Working document invokes Article 179(1) TFEU (European Research Area) and Article 13 of the Charter (freedom of scientific research) as normative anchors for the amendment. However, these references do not clarify the *limits of scientific* research, in light of Article 8(2) of the Charter. Freedom of research does not negate the requirement that interference with data protection must be provided for by law, pursue legitimate aims, and comply with the principle of necessity and proportionality (Article 52(1) of the Charter). Therefore, any legislative amendment to the GDPR affecting the research regime would be expected to explicitly address the conditions under which scientific research can justify restrictions on the right to personal data.

In that regard, the sole reference to compliance with 'ethical standards' does not meaningfully delineate the limits of research. Instead, it risks delegating the determination of those limits

¹⁰² 'Bonn Declaration on Freedom of Scientific Research' 1
<https://www.bmfr.bund.de/SharedDocs/Downloads/EN/b/bonn_declaration_en.pdf?__blob=publicationFile&v=5>
accessed 6 March 2026.

to private or sectoral bodies, thereby raising concerns under Article 52(1) of the Charter, which requires that limitations on fundamental rights be laid down by law.

The proposed reform does not merely amend the definition of scientific research; it recalibrates the counterbalances to establish legality and proportionality embedded in Article 89 GDPR. Under the current architecture, research constitutes a carefully circumscribed regime of conditional derogations. Article 89 integrates research within the GDPR's broader logic by subjecting it to appropriate safeguards, technical and organisational constraints, and, where applicable, national legislative balancing. Research is thus not an autonomous exemption, but a structurally embedded exception reconciled with Articles 5 and 6 GDPR and, ultimately, Article 8(2) of the Charter.

By broadening the notion of scientific research without clarifying its preconditions, the proposal risks transforming this conditional regime into a general gateway for exemptions from core principles, including purpose limitation, storage limitation, transparency obligations, and certain data subject rights, which will be further tackled below under the relevant articles. As emphasised by the European Data Protection Board and the European Data Protection Supervisor in Joint Opinion 2/2026, a definition of scientific research functions as a systemic trigger for derogations under Articles 5(1)(b) and (e), 14(5)(b), 17(3)(d), 21(6) and 89 GDPR, among others.¹⁰³ Therefore, a broad definition has several consequences. It alters the scope of multiple safeguards simultaneously. As a result, it shifts the structural balance originally struck by the legislator in 2016. It is important to carefully consider that a definitional clarification operates as a redistribution of normative weight between data subject rights and research privileges.

Furthermore, the amendment also interacts with the foundational requirement of current valid legal basis under Articles 5(1)(a), 6(1), and, where applicable, 9(2) GDPR. The recital 32 of the proposed amendment suggests that 'the processing of personal data for the purpose of scientific research therefore *pursues a legitimate interest* within the meaning of Article 6(1)(f) of Regulation (EU) 2016/679, provided that such research is not contrary to Union or Member State law.' (emphasis added). In their Joint Opinion, the EDPB and the EDPS support the clarification that scientific research may pursue a legitimate interest under Article 6(1)(f) GDPR, while expressly underlining that all other requirements remain fully applicable. Crucially, they recommend clarifying that, in certain cases, a legal basis other than Article 6(1)(f) may be appropriate for research processing.¹⁰⁴

This observation acquires particular constitutional significance in the context of secondary use. Where personal data are repurposed for research, the original legal basis may not automatically extend to the new purpose. Therefore, 'the question of compatibility of purposes should not be confused with the principle of lawfulness under the GDPR and EUDPR'.¹⁰⁵ The new amendment read in light of recital 32, risks transforming scientific research into an umbrella category capable of absorbing heterogeneous innovation-oriented processing activities and treating them as lawful per se on the basis of a legitimate interest.

Despite the proposal's impact on several fundamental rights, no public consultation or impact assessment has systematically examined how the broadened definition interacts with the

¹⁰³ European Data Protection Board (EDPB) and European Data Protection Supervisor (EDPS), 'Joint Opinion 2/2026 on the Proposal for a Regulation as Regards the Simplification of the Digital Legislative Framework (Digital Omnibus)' (n 78) para 28.

¹⁰⁴ *ibid* 15, para 35.

¹⁰⁵ *ibid* 32.

purpose limitation principle, the requirement of legal certainty, and the proportionality test under Article 52(1) of the Charter. In conclusion, the proposal does not provide a sufficiently substantiated justification demonstrating that the revised definition meets the research community's need for clarification while preserving the structural balance between research privileges and data subject rights embedded in the GDPR architecture.

Problem 3: By eliminating compatibility assessment requirement for further processing for scientific research (as well as for archiving, historical research or statistical purposes), the proposed amendment enables a wide range of incompatible data processing activities

The Digital Omnibus Proposal suggests a new wording for Article 5(1)(b) and thus removes the necessity of the compatibility assessment for further processing mandated under Article 6(4) for archiving, scientific and historical research or statistical purposes. According to the new wording, such processing will be automatically considered to be compatible with the original processing.

Considering the broadened scope of “scientific research” via the addition of a new definition in Article 4(38), this change would enable a significant number of different incompatible processing activities to be undertaken by data controllers, merely on the basis that such activities may be able to support technological development and demonstration. If the purpose of this change is to enable more innovation via removing barriers in front of scientific research, the removal of compatibility assessment requirement is not necessary, because the compatibility assessment as mandated under Article 6(4) does not categorically prevent scientific research or other wider research and development activities. On the contrary, it can be argued that the requirements of the compatibility assessment ensure compliance with the data protection principles under Article 5(1), strengthening compliance of various scientific research as well as wider research and development activities.

Recommendations

We recommend removing the definition of scientific research and instead include a reference to the UNESCO framework through a recital, thereby adhering to universally accepted definitions of science, scientific research and innovation (i.e. whether or not they are part of experimental innovation). This approach would serve to achieve the Digital Omnibus Proposal's alleged goal of the clarifying the notion of ‘scientific research’. Consequently, it would avoid fragmentation while simultaneously preventing function creep of the ensuing derogatory regime.

The proposal must restructure the legal basis implications of research processing, particularly in cases of secondary use. Legislative clarification should not affirm that reliance on Article 6(1)(f) GDPR is automatic and should not exclude other grounds of legal bases. The current system shall be kept where alternative legal bases for research under Article 6(1) can be considered.

It is crucial that the conditional logic of Article 89 is carefully considered and the balance in the GDPR for a scientific research regime is maintained. Research-related derogations should remain exceptional, demonstrably necessary, and subject to effective safeguards. Any recalibration of this regime must be accompanied by a structured proportionality analysis under Article 52(1) of the Charter. It means that before any future proposal, a dedicated impact assessment and public consultation must systematically examine the horizontal effects of the revised definition across the GDPR, its interaction with national implementing

legislation, and its compatibility with Articles 8(2) and 52(1) of the Charter. Given the systemic and constitutional implications, the proposal on scientific research and the requirement on removal of the compatibility requirement should not be accepted.

2.3 The new processing ground for special categories of personal data for AI training and development

According to recital 33 of the Digital Omnibus Proposal, this new derogation aims to enable the processing of special categories of personal data where such data may be incidentally present in datasets and where the processing of such data is not necessary for the main purpose of training, testing or validation of AI systems or models. In practice, it may be disproportionately difficult to identify and remove special categories of personal data that are present in negligible quantities in the large datasets used for the development of AI systems or models. In the absence of another applicable derogation under Article 9(2), the mere possibility of the unintended presence of such data may prevent the use of large datasets in the training, testing or validation of AI systems or models. This could become a barrier, especially for small or medium-sized developers who may not have the capability to identify and remove such incidental sensitive data from large datasets. The proposed amendment is helpful in this context.

However, the actual wording of the proposed derogation fails to clearly reflect the focus on incidental, unintended presence of sensitive data in large datasets. With its current wording, there is a risk that the derogation may be interpreted as enabling much broader data processing in the context of the training, testing or validation of AI systems or models. Moreover, the wording of the derogation uses the phrase “the development and operation [of an AI system]” instead of “training, testing or validation”. As expressed in the joint opinion by the EDPB and EDPS,¹⁰⁶ the inclusion of the word “operation” increases the risk of broader sensitive data processing, which, according to recital 33, is not the aim of the proposed derogation.

Recommendation

The proposed provision should not be accepted in its current form. It should clearly define the limits of the derogation, particularly concerning the incidental and unintended presence of **sensitive data in large datasets used for AI training, testing, and validation.**

2.4 The new processing ground for biometric data

The Digital Omnibus Proposal introduces a specific exception from the general prohibition on processing special categories of personal data, for the purposes of biometric verification. It aims to amend Article 9 of the GDPR (and Article 10 of the EUDPR) to allow processing of biometric data when it is necessary for confirming the identity of a data subject, which, according to the proposal, refers to biometric verification. This is subject to the condition that the “biometric data” or the “means” required for the verification are under the sole control of the data subject.

As further explained in recital 34, this would mean that biometric templates could be stored on the data subject’s device via a secure enclave or trusted execution environment. In this case, the controller would not have access to the template (stored biometric reference) itself, but rather a verification token. Alternatively, the templates could be encrypted and stored by

¹⁰⁶ Ibid 18.

the controller, provided that the data subject holds the encryption key or equivalent means. The controller can only access the biometric data for a very brief time in order to carry out the verification process.

Problem 1: The proposed change overlooks the technical specificities of biometric recognition technologies.

The proposal justifies the change based on the technical distinction between two types of biometric processing: identification and verification. Biometric identification is defined as a "one-to-many" search of a person's biometric data within a database. Biometric verification is defined as a "one-to-one" comparison where a data subject provides biometric data to claim their identity.

The changes proposed neglect the technical reality behind how biometric functionalities work. First, the derogation appears to be narrowly framed around biometric verification understood as one-to-one (1:1) comparison. While the Commission focuses on the comparison phase, the technical standards (ISO) note that many systems perform a "one-to-many" search process to achieve what is legally considered a 1:1 comparison.¹⁰⁷ The AI Act adopted the same 1:1 narrative as in this proposal, which has raised criticisms.¹⁰⁸

Under this reading, biometric search, particularly deduplication checks conducted at enrolment to prevent multiple accounts or identity fraud, would fall outside the scope of the provision. Deduplication inherently requires one-to-many (1:N) comparisons and necessitates that biometric templates be accessible to the controller, meaning they cannot remain under the *sole control of the data subject*. As a result, a technically necessary step for fraud prevention in many biometric verification systems would not benefit from the derogation.¹⁰⁹ In practice, this means that controllers deploying biometric verification systems may still need to rely on multiple derogations under Article 9 GDPR to enrol and verify the claimed identity. This might fragment the legal basis for processing and weaken the GDPR's technology-neutral approach.

Biometric data's highly sensitive nature is ignored in the Digital Omnibus Proposal, which allows a highly broad scope of exception to apply to biometric verification. The proposed new derogation in Article 9(2)(l) allows the processing of biometric data where it is "**necessary for the purpose** of confirming the identity of a data subject (verification)". We think a very broad derogation, such as "necessity" does not correspond to the risks biometric data processing, which are discussed under Problem 3.

Problem 2: Current definition(s) of biometric data across the EU regulatory framework is currently not harmonised and the GDPR definition, along with the current exceptions in Article 9(2) is too narrow to provide protection to fundamental rights and freedoms. The Digital Omnibus Proposal misses the opportunity to broaden protection and achieve harmonisation across regulatory instruments.

¹⁰⁷ 'ISO/IEC 2382-37:2022' (ISO) <<https://www.iso.org/standard/73514.html>> accessed 6 March 2026.

¹⁰⁸ B Sumer, 'The AI Act's Exclusion of Biometric Verification: Minimal Risk by Design and Default?' (2024) 10 European Data Protection Law Review 150 <<https://doi.org/10.21552/edpl/2024/2/6>>.

¹⁰⁹ Carolyn Allen, 'Verification (1:1) and Identification (1:N) Explanatory Graphics' (Biometrics Institute, 16 February 2024) <<https://www.biometricsinstitute.org/verification-11-and-identification-1n-explanatory-graphics/>> accessed 6 March 2026.

One of the pressing problems with biometric data regulation in the EU is the ambiguity of definitions, leading to regulatory inconsistency and legal uncertainty. The GDPR definition of biometric data, and thus, the legal regime for biometric data, is specifically criticised for its narrow scope.¹¹⁰ The definition requires that data result from "specific technical processing" to be considered biometric. This phrase is not defined and creates confusion, regarding the point at which data falls into the more protective sensitive regime in Article 9. A major problem with the definition is that the GDPR definition covers only data used to allow or confirm the unique identification of a person, which creates several loopholes, including partial protection (ignoring risks of function creep).¹¹¹ It clearly excludes the images of biometric characteristics, such as facial images (recital 57).¹¹² Eventually, it creates a separate, more narrow identification regime that governs the GDPR's definition of personal data.¹¹³

Problem 3: The proposal argues that verification under the sole control of the data subject is unlikely to create significant risks to fundamental rights, as under these conditions, the controller does not gain knowledge of the biometric data or only does so for a very limited time during the actual verification process. However, the proposal neglects serious threats to fundamental rights.

As mentioned, under Problem 1, the legal distinction between biometric functionalities is technically flawed and fails to account for reality, including systematic overlaps between biometric identification and verification. As a result of this reading, several hidden risks, including algorithmic bias and discrimination, systematic surveillance and function creep, identity fraud based on deepfakes and the lack of rigorous testing of biometric verification systems, are neglected.¹¹⁴ More importantly, these systems are difficult to contest for individuals as the existence of biometric data for identity verification is often perceived as an "objective source of truth".¹¹⁵

It should be noted that this reasoning of the Commission is in contrast with the EDPB in its Guidelines on Facial Recognition, where it is stated that biometric data processing for verification is perceived equally risky for fundamental rights and freedoms.¹¹⁶ As a risk-based regulation, the GDPR should take into account the actual risks of biometric verification

¹¹⁰ Bilgesu Sumer, 'When Do the Images of Biometric Characteristics Qualify as Special Categories of Data Under the GDPR? A Systemic Approach to Biometric Data Processing' *2022 International Conference of the Biometrics Special Interest Group (BIOSIG)* (2022) <<https://doi.org/10.1109/BIOSIG55365.2022.9897034>> accessed 6 March 2026; Catherine Jasserand, 'Legal Nature of Biometric Data: From "Generic" Personal Data to Sensitive Data' (2016) 2 *European Data Protection Law Review* <<https://doi.org/10.21552/EDPL/2016/3/6>>; EJ Kindt, 'Having Yes, Using No? About the New Legal Regime for Biometric Data' (2018) 34 *Computer Law & Security Review* 523 <<https://doi.org/10.1016/j.clsr.2017.11.004>>.

¹¹¹ Bilgesu Sumer and others, 'AI Acts' Ripple Effect on Biometric Data: Harmonising or Fragmenting the Regulation of Biometric Data' in Kostina Prifti and others (eds), *Digital Governance: Confronting the Challenges Posed by Artificial Intelligence* (TMC Asser Press 2024) <https://doi.org/10.1007/978-94-6265-639-0_8>.

¹¹² Sumer (n 110).

¹¹³ Cesar Augusto Fontanillo Lopez, 'Against Biometric Identifiability: Part I: The Law of What Is Reasonably Likely' (2026) 11 *European Data Protection Law Review* 465 <<https://doi.org/10.21552/edpl/2025/4/10>>.

¹¹⁴ Sumer (n 108).

¹¹⁵ Aaron K Martin and Edgar A Whitley, 'Fixing Identity? Biometrics and the Tensions of Material Practices' (2013) 35 *Media, Culture & Society* 52 <<https://doi.org/10.1177/0163443712464558>>.

¹¹⁶ The guidelines mainly concern law enforcement but touches upon the GDPR as well. See European Data Protection Board (EDPB), 'Guidelines 05/2022 on the Use of Facial Recognition Technology in the Area of Law Enforcement (Version 2.0)' (2023).

systems. The risks might even be exacerbated, by the fact that the biometric verification systems are excluded from the high risk and safety regime of the AI Act.

Recommendation

We recommend that the current Article 9 should apply to both identification and verification functionalities. Biometric data, whether for identification or verification, should not be processed on the ground of broad “necessity” as a legal basis, determined solely by the controller. Biometric data definition needs to be clarified considering the objectives of the GDPR and in light of the risk-based approach, rather than practical considerations. Such a definition needs to explicitly clarify the scope of the derogation to include biometric identification steps that are technically necessary for verification, such as deduplication. The proposed provision needs to be reformulated to incorporate a functional criterion such as necessity for “fraud prevention” rather than relying solely on a rigid verification/identification distinction.

2.5 Abuse of data subject rights

The Digital Omnibus Proposal introduces several amendments in relation to Article 12(5) GDPR.¹¹⁷ Before examining these changes in detail, however, some broader considerations should be recalled. The GDPR aims to ensure a consistent and high level of protection of natural persons within the Union, as well as to strengthen and set out in detail the rights of data subjects.¹¹⁸ To achieve this objective, Chapter III of the GDPR sets out a comprehensive catalogue of rights, including the right of access under Article 15. In this context, it is particularly significant that the right of access is expressly enshrined in Article 8(2) of the EU Charter of Fundamental Rights, as an essential component of the fundamental right to the protection of personal data.¹¹⁹ Moreover, the rights in Chapter III of the GDPR are also rooted in Article 9 of Convention 108, and the level of protection afforded by the GDPR should in no event fall below that guaranteed by the Convention 108.¹²⁰

Problem 1: The example of an excessive request in Article 12(5) GDPR that the data subject abuses the rights conferred by this regulation for purposes other than the protection of their data is formulated in too broad terms.

First, considering its fundamental role to facilitate transparency and its specific inclusion in the EU Charter, the right of access is part of the essence of the right to the protection of personal data. Within the structure of the GDPR, the right of access constitutes a core provision and serves as the entry point to other rights under the GDPR. With the information and/or a copy of their personal data obtained through such a request, data subjects can, where necessary, exercise their other rights under the GDPR. Any limitations on its exercise must therefore be interpreted restrictively.¹²¹ This is particularly true with respect to the

¹¹⁷ European Commission, ‘Digital Omnibus’ (n 30) 56.

¹¹⁸ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4/5/2016) recital 10-11.

¹¹⁹ Charter of Fundamental Rights of the European Union (OJ C 326/392, 26/10/2012).

¹²⁰ Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981 (European Treaty Series - No 108).

¹²¹ EDPB, ‘Guidelines 01/2022 on Data Subject Rights - Right of Access’ para 175 <https://www.edpb.europa.eu/system/files/2023-04/edpb_guidelines_202201_data_subject_rights_access_v2_en.pdf> accessed 2 March 2026.

concept of abuse of rights, which presupposes the exercise of a right in a manner that manifestly exceeds the limits of how a prudent and cautious person would exercise that right.

Second, given the fundamental role of the right of access in the protection of personal data, the CJEU and national data protection authorities/courts have only established an abuse of rights in relation to the right of access in highly specific circumstances. In the context of labour disputes, national courts and data protection authorities have repeatedly affirmed that the right of access cannot be limited to a particular purpose and may be exercised as well for purposes unrelated to data protection. Neither Article 15 nor Article 12 GDPR requires a data subject to state a reason when exercising the right of access. It is clear that the mere fact that a data subject might use this information in a separate labour procedure against the controller does not, in itself, constitute an abuse of rights.¹²² Abuse of rights has been found only in exceptional circumstances. For example, where the procedural conduct demonstrated that the right of access was exercised in such an unreasonable manner vis-à-vis the controllers that the only plausible underlying objective was to subsequently challenge the failure to respond (or to respond in time), with a view to obtaining penalty payments.¹²³ In other cases, national courts have established an abuse of rights where the right of access was exercised solely for the purpose of obtaining information in order to challenge proceedings.¹²⁴

More importantly, an abuse of rights has also already been addressed in the case law of the CJEU. In *FT v. DW*, the CJEU ruled on whether a controller should provide a copy of personal data even where the reason for the request is not one of the reasons referred to in recital 63 GDPR. The CJEU recalled that neither Article 15 nor Article 12 GDPR requires a data subject to state a reason when exercising the right of access.¹²⁵ Accordingly, recital 63 GDPR cannot be interpreted as requiring a request to be refused merely because it pursues a purpose other than verifying the lawfulness of the processing.¹²⁶ The mere existence of another purpose is therefore insufficient to reject the request. In the context of complaints before national data protection authorities, the CJEU ruled in *Österreichische Datenschutzbehörde v. FR* on whether the fact that a complaint has been sent in large number is sufficient to be classified as excessive in the context of Article 57(4) GDPR or whether an abusive intention is necessary to come to such a conclusion. The CJEU concluded that the existence of intentional abuse should be demonstrated taking into account the particular circumstances of the case, for example when the number of complaints is intended to interfere with the proper functioning of the supervisory authority by taking up its resources in an abusive manner.¹²⁷

The abovementioned case law of the CJEU and the decisional practice of national data protection authorities and courts supports the view that the fundamental right to data protection is instrumental to the exercise of other fundamental rights. The data subject right of access plays a crucial role therein.

¹²² [2025] BGH I ZR 115/25; [2025] LAG München 2 SLa 70/25; *Decision 41/2025* [2025] Greek Data Protection Authority 41/2025; [2021] Rb Rotterdam ROT 19/5030, ECLI:NL:RBROT:2021:2306; [2020] AG Kerpen 106 C 96/20; EDPB (n 121).

¹²³ [2022] Raad van State 202006960/1/A3 ECLI:NL:RVS:2022:2403; [2022] Rechtbank Zeeland-West-Brabant AWB- 21_1058 ECLI:NL:RBZWB:2022:5975; [2021] Rb Limburg ECLI:NL:RBLIM:2021:2946.

¹²⁴ [2024] OLG Düsseldorf 6 U 114/23; [2022] LG Gießen 2 O 186/22; [2023] Landesrechtsportal Brandenburg 11 U 332/22 ECLI:DE:OLGDB:2023:0929.11U332.22.00.

¹²⁵ *FT (Copies du dossier médical)* [2023] ECJ Case C-307/22 ECLI:EU:C:2023:811 para 38.

¹²⁶ *ibid* para 51.

¹²⁷ *Österreichische Datenschutzbehörde v FR* [2025] ECJ Case C-416/23 ECLI:EU:C:2025:3 paras 55-56.

Furthermore, the manner in which the abuse of rights is included in Article 12(5) of the GDPR, the Digital Omnibus Proposal gives rise to a risk of misuse, in particular that the abuse of rights exception may be interpreted too broadly. The provision could be read as allowing a controller to refuse a request for access solely on the ground that it pursues a purpose unrelated to data protection, even where that purpose exists alongside a data protection-related objective. Such an interpretation would run counter to the very essence of the right of access, as well as to established case law and decision-making practice.¹²⁸ As acknowledged in recital 35 of the Digital Omnibus Proposal and the Working Staff Document of the Commission restrictions on the right of access should not be abused by the controller.¹²⁹

In conclusion, the mere existence of a purpose unrelated to data protection does not, in itself, render the exercise of the right of access abusive. A purpose unrelated to data protection might exist alongside a purpose related to data protection, as recognized both in the case law of the CJEU and in decisional practice of national courts and data protection authorities. Notably, the examples of abuse of rights in the context of the right of access, which are currently included in recital 35 of the Digital Omnibus Proposal and the Commissions' Working Staff Document¹³⁰ are derived from this decisional practice of data protection authorities and national courts, or are already reflected in the EDPB Guidelines on the right of access¹³¹. As such, the Omnibus Proposal does not appear to be intended to further develop existing case law or established decisional practice.

Problem 2: The requirement in Article 12(5) of the Digital Omnibus Proposal for controllers to prove that there are reasonable grounds to believe that a request is excessive is unclear.

The Digital Omnibus Proposal lowers the burden of proof for controllers for refusing excessive requests, as compared to manifestly unfounded requests. In the case of excessive requests, it would suffice for the controller to demonstrate that there are reasonable grounds to believe that the request is excessive. As indicated in recital 35 of the Digital Omnibus Proposal, we may acknowledge the practical difficulty that potentially abusive conduct by a data subject often lies largely outside the controller's sphere of influence, making it not straightforward for the controller to substantiate such abuse. However, the proposed solution allowing controllers to prove abusive conduct only to a reasonable level is framed in overly broad and ambiguous terms. It remains unclear what it means in practice for a controller to 'prove that there are reasonable grounds to believe' that a request is excessive. As currently drafted, this formulation risks misuse by controllers, who may too easily reject requests on the basis of a low evidentiary threshold. In this regard, the EDPB and the EDPS have expressed doubts as to whether the inclusion of the notion of 'reasonable grounds to believe' would maintain the same high level of protection for individuals or achieve the objective of simplification.¹³²

Second, this approach insufficiently accounts for the position of data subjects. In many contexts, particularly in employment relationships, data subjects are in a structurally vulnerable position. In such contexts, the right of access, portability, and not to be subject to

¹²⁸ European Commission, 'SWF Digital Omnibus' (n 27) 40.

¹²⁹ *ibid.*

¹³⁰ European Commission, 'SWF Digital Omnibus' (n 27) 40.

¹³¹ EDPB (n 121).

¹³² European Data Protection Board (EDPB) and European Data Protection Supervisor (EDPS), 'Joint Opinion 2/2026 on the Proposal for a Regulation as Regards the Simplification of the Digital Legislative Framework (Digital Omnibus)' (n 78) para 57.

automated decision-making have been proven essential in strengthening their position.¹³³ At the same time, controllers have repeatedly tried to refuse such requests by invoking an alleged abuse of rights. By lowering the burden of proof for controllers, the Digital Omnibus Proposal in fact expands the grounds on which access requests may be rejected, thereby making it easier for controllers to refuse access precisely in such vulnerable contexts.

Problem 3: The specification in recital 35 of the Digital Omnibus Proposal that overly broad and insufficiently specified requests may be refused is formulated in overly broad terms.

By simply allowing controllers to refuse requests that are formulated in an overly broad manner, the Digital Omnibus Proposal fails to adequately account for the complexity of multiple and diverse processing activities. Considering the vulnerable position of data subjects, it may be particularly difficult for them to understand which specific processing activities and which supplementary information they wish to access. Allowing the controller to refuse to answer such a request, is overly simplistic and creates a risk of abuse. At the same time, it must be acknowledged that where requests are genuinely excessively broad or vague, controllers cannot reasonably be expected to examine every possible processing activity. In such circumstances, asking for further clarification is justified. However, a refusal requires a careful and proportionate balancing exercise, which is insufficiently reflected in the wording of the proposal.

Problem 4: The proposed revisions are inconsistent with other instruments of EU data legislation.

The proposed revisions introduced by the Digital Omnibus Proposal also raise issues related to the consistency of the GDPR with other data legislations and especially the Data Act, the DGA and the Health Data Space Regulation. Both the Data Act and the Health Data Space Regulation provide new data rights to individuals, as data subjects, that are deemed to go beyond (i.e. in terms of scope, usability of the data, etc.) the GDPR right of access and, respectively, the right to data portability. These rights are intended to enhance individuals' control over their data and enable them to perform actions relating to their data, such as connected products repair, information generation or sleeping patterns (Chapter II of the Data Act). As for the DGA, it sets out the conditions under which individuals can share personal data with third parties, based on their GDPR rights, through the support of trustworthy intermediaries. In other words, data subjects' rights (and especially the right of access) are put as the legal infrastructure for further data sharing, regardless of the subsequent purpose of processing. Whether this architecture is compliant with the GDPR is debatable.¹³⁴ In any case, such recent instruments of EU data legislation are manifestly and fundamentally based on the principle that individuals, shall be entitled and even incentivized to use their data subject rights under the GDPR. Therefore, the proposal risks exacerbating the inconsistencies amongst EU data-related legislations.

Recommendations

We recommend rejecting the proposed provision, as it does not align with existing case law and practice, and it risks enabling excessive intervention in the right of access.

¹³³ See for example [2021] Rb Amsterdam C/13/687315 / HA RK 20-207 ECLI:NL:RBAMS:2021:1020 ECLI:NL:RBAMS:2021:1020; [2021] Rb Amsterdam C/13/689705 / HA RK 20-258 ECLI:NL:RBAMS:2021:1019.

¹³⁴ See in particular, Ducuing, *Data Commodification and the Law: Navigating Data Markets and Data Protection* (n 56).

It should be taken into account that recital 4 of the GDPR already provides explanations for invoking abuse of rights in the context of the right of access. Recital 4 GDPR specifies that the right to the protection of personal data is not absolute, but must be balanced against other fundamental rights, freedoms, and principles recognised by the Charter and enshrined in the Treaties. Both the EU Charter of Fundamental Rights and the European Convention of Human Rights explicitly enshrine the prohibition of the abuse of rights.¹³⁵ Moreover, it is a general legal principle that EU law cannot be relied upon for abusive ends.¹³⁶ In this respect, it might be more useful to issue guidance with more concrete examples on the basis of prior cases to assist on what constitutes an abuse of right, instead of changing the content of the Article 12 (5) of the GDPR.

We further recommend deleting the specification in recital 35 of the Digital Omnibus Proposal which allows overly broad and unspecified requests to be refused. Instead, it would be preferable for controllers to invite data subjects to clarify which information or processing activities their request relates to, in line with recital 63 GDPR. In this regard, we fully agree with the position of the EDPB and EDPS in their Joint Opinion.¹³⁷ Where it is not clear which personal data or information is being requested, controllers should provide an overview of the personal data and information listed in the GDPR, e.g. by referring to (a specific part of) the privacy notice.

2.6 New exemptions for transparency

The right to be informed constitutes an essential part of the right to data protection, established under Article 8 of the Charter of Fundamental Rights of the European Union.¹³⁸ Considering that Article 8 wording includes key data protection principles such as fairness, purpose specification, lawfulness and the rights of access and to rectification, scholars claim that a teleological reading of the Charter suggests that the processing of personal data should be accompanied by robust transparency standards.¹³⁹ The GDPR, therefore, comes in as a tool, establishing operational aspects of these standards.

Additionally, the principle of transparency and related obligations in the context of personal data protection are not only embedded in the EU framework but also constitutes an international consensus. For example, Convention 108+¹⁴⁰ includes a separate Article 8, establishing rules for transparency of processing. As the GDPR is generally seen as the most rigorous privacy standard globally, the level of data protection under the GDPR, including

¹³⁵ Charter of Fundamental Rights of the European Union (OJ C 326/392, 26/10/2012); European Convention on Human Rights 1950.

¹³⁶ *VK and Others v BMW Bank GmbH and Others* [2023] Court of Justice Joined Cases C-38/21, C-47/21, C-232/21, ECLI:EU:C:2023:1014 para 281.

¹³⁷ European Data Protection Board (EDPB) and European Data Protection Supervisor (EDPS), 'Joint Opinion 2/2026 on the Proposal for a Regulation as Regards the Simplification of the Digital Legislative Framework (Digital Omnibus)' (n 78) para 56.

¹³⁸ EU Charter of Fundamental Rights.

¹³⁹ Laurens Naudts, Pierre Dewitte and Jef Ausloos, 'Meaningful Transparency Through Data Rights: A Multidimensional Analysis' *Research Handbook on EU Data Protection Law* (Edward Elgar Publishing 2022) 130; Damian Clifford and Jef Ausloos, 'Data Protection and the Role of Fairness'; Serge Gutwirth and Paul De Hert, 'Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power' (2021) 18 *Direito Público* <<https://doi.org/10.11117/rdp.v18i100.6200>> accessed 13 March 2026; Jef Ausloos, Réne Mahieu and Michael Veale, 'Getting Data Subject Rights Right: A Submission to the European Data Protection Board from International Data Rights Academics, to Inform Regulatory Guidance' (2019) 10 *Journal of Intellectual Property, Information Technology and E-Commerce Law* (JIPITEC) 283 <<https://doi.org/https://nbn-resolving.de/urn:nbn:de:0009-29-50315>>.

¹⁴⁰ Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 223) 2018.

transparency obligations, in no way should be lower than guaranteed by international legal instruments.

Considering the above, any amendment to Article 13 of the GDPR, establishing the right to be informed when data is collected directly from data subjects, must be introduced with extreme cautiousness and careful deliberation.

2.6.1 Article 13(4) of the GDPR

While the intention to reduce the burden on small operators of producing lengthy privacy policies merely to demonstrate accountability is welcomed, the approach proposed in the Digital Omnibus Proposal is underdeveloped and fails to address key transparency concerns.

Problem 1: The proposed wording of Article 13(4) introduces evaluative criteria for the application of the exception that are not sufficiently defined and, therefore, creates legal uncertainty.

The proposed evaluative criteria – (1) ‘clear and circumscribed relationship’, (2) ‘activity that is not data-intensive’, (3) ‘reasonable grounds to assume’¹⁴¹ – are not accompanied with sufficient legal definition in the Digital Omnibus Proposal. Such legal uncertainty would make it difficult for data controllers to rely on this exception in a compliant way, as well as for supervisory authorities to enforce these measures in a consistent manner.

In the proposed recital 36 of the Digital Omnibus Proposal,¹⁴² the Commission aims to provide explanation on how to interpret these new concepts; however, fails to do so sufficiently:

- Clear and circumscribed. In the draft recital, the Commission claims that the relationship between a craftsman and his clients is very clear and circumscribed. However, no tangible factors that should be evaluated to determine such a relationship in other cases are provided in the proposal.
- Data-intensive. The Commission claims that the ‘*activity is not data-intensive where it [controller] collects a low amount of personal data and its processing operations are not complex, which is not the case, for example, in the field of employment.*’ The attempted definition of the data-intensive processing includes another evaluative metric – ‘complex’ data processing operations – which again is not described or further explained in the proposal.
- Reasonable grounds to assume. The proposed recital considers that there should be reasonable grounds to assume that the data subject has the sufficient information in cases where data processing is based on contractual necessity or consent and the same would apply to associations and sports clubs. However, again, the draft proposal provides no sufficient explanation on why only the processing based on the contractual basis or consent is included here as a reference.

The CJEU has repeatedly held that legal certainty is a core principle of the EU law. This principle requires for legal rules to be clear and precise, so that individuals can clearly understand their

¹⁴¹ European Commission, ‘Digital Omnibus’ (n 30).

¹⁴² *ibid* recital 36.

rights and obligations and act accordingly.¹⁴³ The proposed amendment of Article 13(4), however, seems to contradict this principle.

The proposed Article 13(4) introduces new concepts into the existing GDPR framework without clearly defining them and proposed recital 36 adds further ambiguity rather than clarity. For example, the recital suggests that employment relationships are always data-intensive but does not address situations involving the processing of special category data. This raises the question of whether such processing could in essence be considered not data intensive and, therefore, fall within the proposed exception. The draft recital also suggests that sports clubs automatically meet the requirement of having reasonable grounds to assume that data subjects are sufficiently informed. However, many sports clubs use fingerprint-based access systems, which involve the processing of biometric data and GDPR fines have already been issued for non-compliance with such processing.¹⁴⁴ In these circumstances, it is unclear whether consent to the use of fingerprints could even be validly obtained without providing the full information required under Article 13.

As the article is drafted ambiguously and the proposal lacks an explanatory recital, with the adoption of a current version, controllers, who want to rely on this exception, will have to put additional resources to evaluate and guess for themselves whether the proposed criteria are met. At the same time, supervisory authorities will be asked to enforce the new obligation without a clear understanding of how those new criteria are meant to work in practice.

Recommendations

As a reminder, the version proposed with the Digital Omnibus Proposal is meant to replace the current version of Article 13(4) of the GDPR where the controller is allowed not to provide information under Article 13 where and insofar the data subject has this information.¹⁴⁵ Adoption of the current proposal would mean that controllers would be extremely limited to use the exceptions and at the same time would be deprived of the current possibility to use the obvious exception. Furthermore, the mentioned Convention 108+ includes this obvious exception (Article 8(2)),¹⁴⁶ so its exclusion from the GDPR would be illogical and incompatible with international standards. As an additional reference, the current Article 14(5) of the GDPR already includes both: the exception where the data subject already has information and additional exceptions based on the specific circumstances. If the Commission rethinks and proposes the functional and proportionate criteria to be applicable for the exception under Article 13(4), a similar approach to the one established under Article 14(5) should be taken.

It must be noted that the leaked Council's file¹⁴⁷ on compromise text of the Digital Omnibus Proposal addresses certain issues raised in this section. For example, the draft document shows that the Council agrees that the application of derogation should be limited to situations where the controller can objectively demonstrate that the data subject already

¹⁴³ Paul Craig, 'Legal Certainty and Legitimate Expectations' in Paul Craig (ed), *EU Administrative Law* (Oxford University Press 2018) 549–550 <<https://doi.org/10.1093/oso/9780198831655.003.0020>> accessed 5 March 2026.

¹⁴⁴ European Data Protection Board, 'Lithuanian DPA: Fine Imposed on a Sports Club for Infringements of the GDPR in Processing of Fingerprints of the Customers and Employees |' (8 July 2021) <https://www.edpb.europa.eu/news/national-news/2021/lithuanian-dpa-fine-imposed-sports-club-infringements-gdpr-processing_en> accessed 5 March 2026; 'Lithuania: VDAI Fines Praktiskas €6,000 for Unlawful Processing of Personal Data | News' (*DataGuidance*, 13 January 2023) <<https://www.dataguidance.com/news/lithuania-vdai-fines-praktiskas-eu6000-unlawful>> accessed 5 March 2026.

¹⁴⁵ GDPR.

¹⁴⁶ Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981, ETS 108.

¹⁴⁷ Council of the European Union, 'Presidency Compromise Text on Omnibus VII – Digital (GDPR/P2B)' (2026) 6406/26 <https://www.euractiv.com/content/uploads/sites/2/2026/02/EURACTIV_OMNIBUS-1.pdf> accessed 6 March 2026.

possesses the required information and reintroduces the Commission's omitted current version of 'insofar as the data subject has the information'. Instead of 'very clear', 'circumscribed' and 'not data intensive', the Council proposes to include 'direct, limited and clearly circumscribed relationship [...] and is not likely to result in a high risk to the rights and freedoms of data subjects nor involve the processing of large amounts of personal data, special categories of personal data or complex processing operations' (updated recital 36 and Article 13(4)). Additionally, the Council suggests removing some of the ambiguous and unclear explanations in recital 36. This proposed version makes more sense and, at a first glance, poses fewer risks to data subjects' rights – it reinstates the very obvious exception and introduces GDPR-known categories into the exception. However, it does not solve all the issues of the legal uncertainty – e.g., no indication of what direct, limited and clearly circumscribed relationship means is provided, nor it is explained what are 'complex processing operations'. If the Commission maintains the idea of updating Article 13(4), it should further search for the appropriate criteria to apply the exception for small actors – e.g., a deeper analysis and consultation on how to define the listed criteria in clearer terms should be performed. Building on the current Council's working document would be highly advised as it starts to address some of the key issues of the Commission's proposal.

Problem 2: the proposed wording of Article 13(4) introduces exceptions that are difficult to apply in practice and, therefore, fails to achieve its intended purpose

The proposed Article 13(4) foresees four exceptions each constructed with an 'unless' wording – i.e., exceptions of the exception which prove that the proposed exception is hardly usable.

The Commission's staff working document explains that from the proposed Article 13(4) *'would benefit in particular small operators [...] that carry out low-risk data processing to whom information obligations may cause disproportionate burden given that the processing of personal data is not their core activity.'*¹⁴⁸ However, in practice, even if the proposed criteria were unambiguous, the exceptions of the exception proposed would still not allow small operators to lower the administrative burden.

One of the proposed use cases establishes that the exception from the information obligation would not apply when the controller transmits the data to other recipients or categories of recipients.¹⁴⁹ Under Art. 4(9) of the GDPR, the recipient means *'a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not.'*¹⁵⁰ In other words, even if it is a small operator, there is very little chance that the operator does not use e-mail or other IT service provider to which it transfers its client's data.¹⁵¹ Furthermore, this exception does not address what, for example, a craftsman should do if he later in the client relationship decides to move from paper invoices to IT-based solutions. In such a case, the required information was 'legally' not provided at the time of data collection. If the circumstances change, it is unclear whether the craftsman would be required to issue a new privacy notice. Legal loops like this may significantly affect principles of transparency and accountability.

¹⁴⁸ European Commission, 'SWF Digital Omnibus' (n 27) para 1.2.2.6.

¹⁴⁹ European Commission, 'Digital Omnibus' (n 30).

¹⁵⁰ GDPR.

¹⁵¹ NOYB (n 98) 39.

Another use case is hardly operable as well. It claims that the proposed exception does not apply where data is transferred to a third country.¹⁵² If it is transferred to a data recipient, then it already falls under the first exception. If it is meant to be applied in cases where data is transferred within the same company, it is very hard to think of a scenario where a small operator like a craftsman would have servers based outside the EEA. And either way, this would then possibly hardly amount to non-data-intensive data processing.

The two other use cases – automated decision making and the high-risk exceptions – may be understandable as these concepts in the GDPR already require a higher level of cautiousness and additional action to be taken due to the nature of data processing and, therefore, could be a good ground for the exception of an exception. However, the current reference to Article 35 undermines the very goal of simplifying the process of providing information to data subjects. The Digital Omnibus Proposal also puts forward the idea of making a coherent list of the processing operations which are subject to the requirement for a data protection impact under Article 35. However, that does not necessarily resolve the problem, as the definition of ‘is likely to result in a high risk to the rights and freedoms of natural persons’ is not intended to change in the current draft proposal. Under the current practice, to determine whether processing is considered high risk under Article 35, data controllers – including small operators – would still need to carry out an initial assessment. For example, the WP29 guidelines on data protection impact assessments.¹⁵³ list a number of complex factors that must be considered when assessing whether processing is likely to result in a high risk. In practice, with this proposed exception, small operators would still need to assess in depth whether their data processing may amount to high-risk processing and will be burdened with other administrative matters even before deciding whether the proposed exception on providing information to data subjects applies to them.

The leaked Council’s file¹⁵⁴ introduces an additional use case where the exception proposed in Article 13(4) would not apply – i.e., where the controller intends to process the data collected from the data subject for other purposes. This looks like a mere correction to ensure the correlation with the current Article 13(3), which is very welcomed. However, if that is the case, it might simply be easier to exclude the part of the current proposal Article 13(4) which says that paragraph 3 does not apply. In any case, the Council seems to also fail to address the other exceptions that essentially make the Article 13(4) option unusable.

Recommendation

It is necessary to reconsider whether the proposed exceptions do not undermine the overall purpose of the exception in Article 13(4). While these exceptions to the exception are intended to protect data subjects and ensure they are informed when data is further transferred or when high-risk processing occurs, in practice, they make the exception largely inoperable even for the small operators for whom the proposal is intended, as they would be unable to rely on it or would face additional administrative burdens that the proposal aimed to avoid in the first place.

¹⁵² European Commission, ‘Digital Omnibus’ (n 30).

¹⁵³ Article 29 Working Party, ‘Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is “Likely to Result in a High Risk” for the Purposes of Regulation 2016/679’ (2017) wp248rev.01 <<https://ec.europa.eu/newsroom/article29/items/611236>> accessed 5 March 2026.

¹⁵⁴ Council of the European Union (n 147).

Problem 3: The suggested exception lowers the level of transparency and the possibility to exercise data subject rights

In the Staff Working Document, the Commission claims that the proposed amendment ‘would ease the information obligation in situations meeting this obligation would bring no genuine added value to data subjects and could therefore be considered unnecessary.’¹⁵⁵ While the idea is to ensure that data subjects are not overburdened with information where very little data processing in non-privacy intrusive environments happen, the chosen wording does not serve this purpose.

For example, the proposed wording claims that the possibility of not informing data subjects can apply where there are reasonable grounds to assume that the data subject has the information referred to in points (a) and (c) of paragraph 1 of Article 13¹⁵⁶ – i.e., information about the identity and contact details of the controller, contact details of a data protection officer, the purposes of the processing for which the personal data are intended, as well as the legal basis for the processing. However, there is no sufficient evidence provided on why only the elements of a-c of part 1 were chosen and why other elements currently included in Article 13 of the GDPR are ‘less important’ and, therefore, now excluded in the proposed cases.

Furthermore, in the proposed recital 36, the Commission states that such a situation (i.e., the new exception) may be invoked in cases where data processing is based on the contract or consent.¹⁵⁷ However, it is then unclear how fully informed contracts can be concluded or informed consent can be given in the first place without providing sufficient information under Article 13 at the time of data collection. While concluding an informed contract is a commercial law matter, informed consent is a GDPR requirement which needs to be fulfilled.

The biggest drawback, in our view, is that in the described cases under the proposed exception, the data subject will not be provided with information about their rights as currently required under Part 2 of Article 13. This means that for data subjects, the possibility to further use those rights becomes more difficult if sufficient information is not provided at the time of collection of personal data.

In its judgment in *Bara*, the CJEU emphasised that the obligation to inform data subjects about the processing of their personal data is particularly significant, as it directly affects their ability to exercise key data protection rights, including the rights of access, rectification and objection to the processing of their data.¹⁵⁸

The draft recital claims that *‘this derogation from the obligations of Article 13 is without prejudice to the independent obligations of the controller under Article 15 of that Regulation, which applies in case the data subject requests access based on the latter provision.’*¹⁵⁹ As mentioned, this means that where the exception proposed under draft Article 13(4) is relied upon, the data subject is never informed about the possibility to use the right of access.

¹⁵⁵ European Commission, ‘SWF Digital Omnibus’ (n 27) para 1.2.2.6.

¹⁵⁶ European Commission, ‘Digital Omnibus’ (n 30).

¹⁵⁷ *ibid* recital 36.

¹⁵⁸ *Smaranda Bara and Others v Casa Națională de Asigurări de Sănătate and Others* [2015] ECJ Case C-201/14; cited in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020) 422 <<https://doi.org/10.1093/oso/9780198826491.001.0001>> accessed 5 March 2026.

¹⁵⁹ European Commission, ‘Digital Omnibus’ (n 30) recital 36.

Additionally, the current version of the recital related to the proposed Article 13(4) oversees that Article 15 does not include all the information under Article 13 – e.g., the legitimate interest relied on or specific rights that the data subject has (e.g., the right to withdraw consent). Therefore, a data subject would, in theory, be deprived of the possibility to receive all information on certain aspects of the data processing currently guaranteed under the GDPR.

It is very welcomed that the leaked Council's file¹⁶⁰ suggests adding to recital 36 that 'application of the derogation from the information obligation should not undermine the principle of transparency'. However, the Council's suggestions still fail to address key concerns, such as providing data subjects with information about their data subject rights.

Recommendations

Considering all three points – i.e., vague evaluative criteria to apply the proposed exception, exceptions of the exception that prove the proposal essentially inoperable and the lowered level of transparency – the most reasonable approach would be to reject the current Article 13(4) proposal and while not abort the idea itself completely, rethink the overall approach on how to simplify the burden of providing excessive privacy policies, especially for small actors, while maintaining the sufficient level of transparency for data subjects.

In our view, a reasonable approach at the moment would be to give priority to the idea that is currently included in the proposed recital: *'Where the derogation from the obligations of Article 13 does not apply, in order to balance the need for completeness and easy understanding by the data subject, controllers may adopt a layered approach when providing the information required, notably by allowing users to navigate to further information.'*¹⁶¹ The essence on how to simplify transparency obligations without reducing transparency is already there; the Commission is encouraged to build on this.

In addition, more attention should be given to ensure a consistent interpretation of transparency obligations across supervisory authorities. Clear guidance is needed on how information can be provided in a practical and proportionate manner. Such guidance should include what constitutes a sufficient standard for providing information, especially for small operators. The Commission, together with the relevant stakeholders should, therefore, be encouraged to explore additional ways of simplifying the information requirements under Article 13 for small operators, such as the use of standardised privacy policy templates, as suggested by NOYB in the analysis of the Digital Omnibus Proposal.¹⁶²

2.6.2 Article 13(5) of the GDPR

Problem 1: Exception, mirroring the current Article 14(5)(b) exception, does not fully align with the general purpose of Article 13

The proposed Article 13(5) essentially mirrors the current Article 14(5)(b) of the GDPR. According to the WP29 Transparency Guidelines, 'Article 14(5)(b) allows for 3 separate situations where the obligation to provide the information set out in [Article 14] is lifted: (i) where it proves impossible (in particular for archiving, scientific/ historical research or statistical purposes); (ii) where it would involve a disproportionate effort (in particular for

¹⁶⁰ Council of the European Union (n 147).

¹⁶¹ European Commission, 'Digital Omnibus' (n 30) recital 36.

¹⁶² NOYB (n 98) 39.

archiving, scientific/historical research or statistical purposes); or (iii) where providing the information required under Article 14.1 would make the achievement of the objectives of the processing impossible or seriously impair them.¹⁶³

While the wording aims to mirror Article 14(5)(b), it is not fully similar. Under the proposed Article 13(5) the emphasis is put on the scientific research solely, while Article 14(5)(b), as mentioned above, allows for exceptions in other cases too. While the proposed recital 37 reaffirms that the new exception is aimed for scientific research only,¹⁶⁴ without sufficient guidance and following the existing practices, the wording, mirroring Article 14(5)(b), may be interpreted and applied by the supervisory authorities in a broader manner, especially as related to impossibility or serious impairment of objectives of data processing.

In their joint opinion,¹⁶⁵ the EDPB and EDPS support the proposed Article 13(5). The EDPB and EDPS even confirm the necessity of this new addition – e.g., it could be relevant in a ‘case when personal data that were directly collected from data subjects are further processed for scientific research purposes, but the controller has not retained any contact details. Another example is where the provision of information would render impossible or seriously impair the objectives of scientific research.’ However, the EDPB and the EDPS provide an abstract comment without addressing what is the actual practical necessity of the proposed exception.

The proposal to add another exception under Article 13 prompts the question whether it is empirically necessary and under what circumstances such an exception would actually be needed. For example, the Transparency Guidelines emphasise that the ‘impossibility or disproportionate effort typically arises by virtue of circumstances which do not apply if the personal data is collected from the data subject. In other words, the impossibility or disproportionate effort must be directly connected to the fact that the personal data was obtained other than from the data subject.’¹⁶⁶ Therefore, it is hard to see how this approach could have changed without sufficient evidence provided by the Commission.

First, in current empirical research domains (health, social science, etc.) research often relies on secondary datasets,¹⁶⁷ which means, that researchers do not have direct contact with data subjects. Therefore, the transparency exception in research contexts is primarily important under Article 14, not Article 13. Second, even if researchers obtain data directly from data subjects, it is difficult to think of a situation where it would be impossible to further inform subjects about their data processing. For example, in clinical trials or psychological assessments, consent is usually obtained directly, and the researchers already have the necessary information to contact the research subjects to provide them with information on further data processing. Similarly, companies like social media operators can reach out to their own users if they intend to use their data for research purposes. Therefore, if data is obtained directly from data subjects, it is hardly the case that it would be impossible or otherwise

¹⁶³ Article 29 Working Party, ‘Guidelines on Transparency under Regulation 2016/679’ (2017) WP260 rev.01 <https://www.edpb.europa.eu/our-work-tools/our-documents/article-29-working-party-guidelines-transparency-under-regulation_en> accessed 5 March 2026.

¹⁶⁴ European Commission, ‘Digital Omnibus’ (n 30) recital 37.

¹⁶⁵ European Data Protection Board (EDPB) and European Data Protection Supervisor (EDPS), ‘Joint Opinion 2/2026 on the Proposal for a Regulation as Regards the Simplification of the Digital Legislative Framework (Digital Omnibus)’ (n 78) para 33.

¹⁶⁶ Article 29 Working Party (n 163) 30.

¹⁶⁷ European Data Protection Board, ‘Study on the Secondary Use of Personal Data in the Context of Scientific Research’ (2020) EDPS/2019/02-04 <https://www.edpb.europa.eu/system/files/2025-04/20250401_study_on_the_secondary_use_of_personal_data_in_the_context_of_scientific_research_23102020_en.pdf> accessed 6 March 2026.

difficult to inform data subjects about their personal data processing in the same way as is currently established under Article 14(5)(b).

Taking into account the above, the proposed exception does not seem to be practically necessary following the current research practices but would open the doors to applying the exception for unclear research purposes which are aimed to be defined more broadly under the current Digital Omnibus Proposal (see our related comments provided above under the section concerning the definition of scientific research & exception from purpose limitation).

Recommendation

We recommend that the proposed exception under Article 13(5) shall be reviewed considering the proposed changes to the definition of scientific research. It must be ensured that the right to be informed is not undermined merely for the purposes of digital innovation without clarifying the proportionate scope of such exceptions. To adopt the proposed Article 13(5), analysis of the real-life examples where such an exception would prove to be necessary and proportionate must be performed and sufficient proof is to be provided together with the Digital Omnibus Proposal. Current proposal for Article 13(5) which lacks sufficient proof for real life scenarios should be rejected.

2.7 Automated decision-making and profiling

Problem 1: The general right not to be subject to impactful decisions based on automated individual decision-making as per current art. 22(1) is repealed.

The first significant change proposed to Article 22 GDPR concerns the repeal of the right of natural persons not to be subject to *decisions* based *solely* on automated individual decision-making, significantly *affecting them*, as provided by the current Article 22(1).¹⁶⁸ Decisions based *solely* on automated individual decision-making and significantly *affecting natural persons* become overall allowed, where at least one of the three conditions provided by the new provision is met. In essence, the current exceptions of Article 22(2) for the prohibition of Article 22(1) are reformulated as conditions to be respected for automated individual decision-making to take place. At first glance, it may seem that the repeal of the general right not to be subject to automated individual decision-making does not significantly impact the practice, as the current exceptions to this right are extremely broad. In a similar vein, the European Commission states in the Staff Working Document that '*The provision clarifies the circumstances as to when decisions based solely on automated processing are permitted*',¹⁶⁹ without referring by no means to the repeal of the right provided by the current Article 22(1). Nonetheless, from an interpretative and systematic point of view, we argue that the amendment represents a structural shift, where no overarching protection against impactful decisions based on automated individual decision-making is provided.¹⁷⁰

Recommendation

The right not to be subject to automated individual decision-making should be maintained, given its overarching systematic and interpretative function. In this sense we fully support the position expressed by the EDPB-EDPS in their Joint Opinion 2/2026, which recalls that the CJEU

¹⁶⁸ For an explanation of the current scope of article 22(1) see Article 29 Data Protection Working Party, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679' (2018) 17/EN WP251rev.01 20.

¹⁶⁹ European Commission, 'SWF Digital Omnibus' (n 27) 41.

¹⁷⁰ See on this point NOYB (n 98).

interpreted Article 22 as a prohibition with exceptions under specific conditions, conferring a right that data subjects can invoke.¹⁷¹

Moreover, the scope of the right, as currently formulated by Article 22(1), should be clarified. Specifically, the use of the adverb 'solely' has given rise to ambiguity in the interpretation of the norm, as in theory even a minimum presence of human involvement could be considered sufficient to exclude that the decision has been based *solely* on automated decision-making. Instead, the provision should explicitly require a meaningful human involvement in the decision, along the standard established at the interpretative level¹⁷².

Problem 2: The requirement of necessity to "enter or perform a contract" has been emptied of its substance

The second significant change proposed to Article 22 GDPR concerns the condition of necessity to enter/perform a contract. The proposal not only converts the current exception to the right not to be subject to decisions based solely on automated individual decision-making that significantly affect natural persons into a condition under which such processing is permitted but also modifies its scope. The proposed amendment states that the condition is met '*regardless of whether the decision could be taken otherwise than by solely automated means*'.¹⁷³ This means in practice that the controller can always justify a decision taken *solely* by automated processing, even if the type of decision at stake can be viably performed by humans. Recital 38 of the proposal specifies: '*[...] the fact that the decision could also be taken by a human does not prevent the controller from taking the decision by solely automated processing [...]*'.¹⁷⁴

The word 'necessary' would lose all meaning, and a condition based on such an undefined 'necessity' would, in effect, be the same as having no condition. Beyond weakening Article 22 and rendering its protection highly unreliable for data subjects seeking to invoke it, the Omnibus proposal's framing of 'necessity' is in direct conflict with the concept of necessity under EU law, including Article 52(1) of the EU Charter of Fundamental Rights and CJEU case law.¹⁷⁵

As demonstrated by the CJEU in the *Huber* (Case C-524/06, para. 52) and underscored by the EDPB in its official guidelines (Guidelines 2/2019, paras. 23-25), 'necessity' is not a novelty introduced by the GDPR, but an independent concept under Union law with an established meaning. Therefore, the GDPR should utilise, interpret, and apply this concept in the context of personal data protection, rather than fundamentally redefining it. In *Meta v Bundeskartellamt* (Case C-252/21, para. 98), the CJEU considered when processing is necessary for the performance of a contract within the meaning of Art. 6(1)(b) GDPR. The Court established that necessity implies *objective indispensability* for a given purpose *and simultaneously* requires that a data controller must be able to demonstrate how the main contractual subject matter could not *otherwise* have been achieved without the activity in question (in that instance: personal data processing). It is therefore impossible to gauge any

¹⁷¹ European Data Protection Board (EDPB) and European Data Protection Supervisor (EDPS), 'Joint Opinion 2/2026 on the Proposal for a Regulation as Regards the Simplification of the Digital Legislative Framework (Digital Omnibus)' (n 78).

¹⁷² See Article 29 Data Protection Working Party, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679' (2018) 17/EN WP251rev.01; *OQ v Land Hessen* (C-634/21) [2023] ECI C-634/21, ECLI:EU:C:2023:957.

¹⁷³ European Commission, 'Digital Omnibus' (n 29) Article 3(7) and recital 38.

¹⁷⁴ *ibid* recital 38.

¹⁷⁵ As pointed out also by NOYB (n 98).

activity's contractual necessity without considering alternative possibilities offered by other approaches. This is why the necessity test is termed 'strict' in EU data protection law.

The current formulation is likely to incentivise an automation-first approach in impactful decision making without assessing its necessity in detail when controllers enter into or perform contracts with data subjects. This approach is further echoed in the recitals. Recital 38 ends with *"Where several equally effective automated processing solutions exist, the controller should use the less intrusive one."* Framed this way, necessity and proportionality are assessed only among automated options, effectively excluding hybrid, non-automated or manual decision-making from consideration at the outset.

This also elevates the importance of required safeguards for automated individual decision making as enshrined in Article 22(3), which obliges controllers to *"implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision."* Although Article 22(3) remains textually unchanged under the Omnibus proposal, an increased reliance on automated decision-making through contracts is likely to intensify pressure on these safeguards, which are often unavailable or ineffective in practice. This will lead to heightened exposure of data subjects to rights violations and, consequently, increased DPA enforcement actions and judicial scrutiny (e.g., SCHUFA case C-634/21¹⁷⁶). The Omnibus proposal's stipulation that contractual necessity under Article 22 is to be tested "regardless of whether the decision could be taken otherwise than by solely automated means" creates therefore a legal paradox that is incompatible with the principles of necessity and proportionality under Union law (e.g., Article 52(1) CFREU) beyond the context of Article 22. Considering that recital 38 of the Omnibus proposal justifies the Article 22 alterations as a mere "clarification" aimed at providing "greater legal certainty", the fact that the amendments would re-interpret fundamental legal concepts to the detriment of legal certainty calls their appropriateness into question.

Recommendations

The meaning of 'necessary' as a genuine condition for automated individual decision making shall be maintained. The current proposition contradicts with the consolidated CJEU interpretation of the concept of necessity under EU law as (i) *objective indispensability* for a given purpose and (ii) demonstration that the main contractual subject matter could not *otherwise* have been achieved without the automated decision making. **In other words, the condition of necessity must be satisfied by the nature of the decision to be taken, i.e., a task that cannot normally be performed by human beings.**

In this regard we do *not* share the view expressed by the EDPB-EDPS in their Joint Opinion 2/2026, according to which the requirement of necessity is compatible with controllers taking decisions by solely automated means when the same decision could theoretically also be taken by a human.¹⁷⁷

In addition, given the fast-evolving properties of artificial intelligence technologies, with ever increasing autonomy (e.g., agentic AI), and the easiness of justifying automated individual decision making for tasks that cannot normally be performed by human beings, the condition

¹⁷⁶ *OQ v Land Hessen (C-634/21)* (n 172).

¹⁷⁷ 'EDPD-EDPS Joint Opinion 2/2026 On the Proposal for a Regulation as Regards the Simplification of the Digital Legislative Framework (Digital Omnibus)' (n 79).

of ‘necessity’ should be scoped narrowly. It could be reasonably confined to the automation of decisions based on parameters pre-identified by the controller and that do not leave a margin of discretion to the automatic decision-making process.

2.8 Cybersecurity and the GDPR (Art. 88a)

Article 88a of the GDPR restructures personal data processing for terminal equipment access under Article 5 of the ePrivacy Directive.¹⁷⁸ It does so by inserting a legal basis for personal data processing related to terminal equipment into the GDPR. It stipulates the conditions of storage and further access to terminal equipment by establishing a general prohibition combined with a closed list of exceptions. Among these, as opposed to Article 5(3) of the EPD¹⁷⁹, Article 88(a)(3)(d) allows access without consent where it is *necessary* for maintaining or restoring the security of a service requested by the data subject or the terminal equipment used to provide that service. The core tension lies in reconciling the increasing need for cybersecurity measures with the historically strong protection afforded to terminal equipment¹⁸⁰ as part of the user’s private sphere. The provision attempts to strike a balance by recognising security needs while confining the exception to a highly sensitive technical layer (device level).

The device-level security exception- The decision to limit the security exception to the terminal equipment level reflects a historical and deliberate choice. It is historical because the processing in relation to the device layer is regulated specifically under the EPD.¹⁸¹ Now, as part of a solution to overlapping framework under the GDPR and EPD, it is inserted under the GDPR. Second, it is deliberate because terminal equipment access is uniquely intrusive as it can expose behavioural data in relation to individuals. At the same time, EU law already provides extensive frameworks for cybersecurity at other levels, notably through Article 32 GDPR for data security and the NIS 2 Directive for systemic and organisational cybersecurity. Article 88a(3)(d) therefore, does not aim to regulate personal data processing for cybersecurity in general, but to permit only those security interactions that are at the endpoint, while preventing cybersecurity from becoming a general justification for bypassing consent.

¹⁷⁸ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L 201/37.; See for the guidelines adopted by the EDPB on Article 5(3), European Data Protection Board, *Guidelines 2/2023 on Technical Scope of Article 5(3) of Directive 2002/58/EC (ePrivacy Directive)* (Version 2.0, 16 October 2024) <https://www.edpb.europa.eu/system/files/2024-10/edpb_guidelines_202302_technical_scope_art_53_eprivacydirective_v2_en_0.pdf> accessed 25 February 2026.

¹⁷⁹ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L 201/37, art 5(3). Article 5(3) does not refer to a security as an exception. So, there will be different regime according to processing of personal or non-personal data as Article 5(3) of the EPD. See for a similar analysis, noyb, *Digital Omnibus: First Analysis of Select GDPR and ePrivacy Proposals by the Commission* (noyb, 2025), p. 65 <<https://noyb.eu/en/digital-omnibus-first-analysis-select-gdpr-and-eprivacy-proposals-commission>> accessed 25 February 2026.

¹⁸⁰ This protection is related to confidentiality of the communication under right to privacy and applies regardless of personal and non-personal data. See Case C-673/17 *Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband eV v Planet49 GmbH* EU:C:2019:801, ECLI:EU:C:2019:801., para. 70.; See the history of cookies and EU law, J Tomisek, ‘Cookies and EU Law: History, Future Regulation and Critique’ (2023) *Technology and Regulation* 35.

¹⁸¹ J Tomisek, ‘Cookies and EU Law: History, Future Regulation and Critique’ (2023) *Technology and Regulation* 35.

Problem: Although Article 88a(3)(d) limits the security exception to necessary access or storage of personal data on terminal equipment, its ambiguous interpretation and application could create significant legal uncertainty and opportunities for misuse.

Article 88a(3)(d) introduces a security exception that is deliberately limited to access to or storage of personal data on terminal equipment where such access is necessary to maintain or restore security. However, several interrelated risks arise from the way this exception may be interpreted and applied in practice.

First, the phrase “service requested by the data subject” is inherently ambiguous in modern digital environments characterised by passive browsing, background app activity, and continuous connectivity. If mere access to a website or application were treated as a “request,” the exception could justify continuous device-level security monitoring, transforming an exception into a default rule.

Second, the use of the term “necessary,” rather than “strictly necessary,”¹⁸² risks diluting the threshold in cybersecurity contexts where preventive measures become a standard practice.¹⁸³

Third, the increasing reliance on anticipatory and preventive security techniques creates the risk that device-level access becomes persistent and continuous.¹⁸⁴ It can result in undermining ‘the prohibition-first’ logic of Article 88a of the GDPR.

Fourth, security-related data obtained from terminal equipment is highly valuable and context-rich. It creates strong incentives for secondary use for analytics, profiling, or optimisation, which threatens the principle of purpose limitation.

Finally, there is a structural tension between data minimisation and cybersecurity, as security often benefits from longitudinal analysis, while Article 88a requires limitations in scope, duration, and data categories.

Taken together, these risks point to a broader risk of interpretation, whereby operational convenience gradually expands the scope of Article 88a(3)(d) beyond its intended function as a narrowly tailored endpoint-security exception.¹⁸⁵

Recommendations

These risks can be addressed through a coherent set of interpretive, architectural, and legislative solutions that preserve both cybersecurity effectiveness and the integrity of consent-based protection.

First, the notion of a “service requested by the data subject” should be interpreted restrictively, referring only to concrete and identifiable functional interactions actively initiated by the user, such as authentication, transaction execution, or form submission, rather

¹⁸² Interestingly, while the EDPB and EDPS Joint Opinion supports the insertion of this exception due the legitimate interest nature of IT security and data protection, it gives the example of ‘strictly’ necessary security updates to provide the context for the exception, see European Data Protection Board (EDPB) and European Data Protection Supervisor (EDPS), ‘Joint Opinion 2/2026 on the Proposal for a Regulation as Regards the Simplification of the Digital Legislative Framework (Digital Omnibus)’ (n 78) para 103.

¹⁸³ See for a general understanding of proactive and preventive cybersecurity techniques, see Rakibul Hasan Chowdhury and others, ‘The Role of Predictive Analytics in Cybersecurity: Detecting and Preventing Threats’ (2024) 23 World Journal of Advanced Research and Reviews 1615 <<https://doi.org/10.30574/wjarr.2024.23.2.2494>>.

¹⁸⁴ See for a similar analysis and the possibility of use of invasive technique under the security exception, NOYB (n 98) 66.

¹⁸⁵ See for a similar analysis based on Article 7 and 8 of the Charter, *ibid*.

than passive exposure or background presence. Second, although the provision uses the term “necessary,” necessity must be assessed contextually and functionally, requiring controllers to demonstrate that the specific security objective cannot reasonably be achieved through less intrusive means, such as server-side controls or aggregated monitoring. Third, device-level security access should be temporally and situationally bounded, remaining lawful only for as long as required to address a specific concrete security risk and ceasing once that function is fulfilled, so that the preventive security measures do not become continuous monitoring.¹⁸⁶ The tension between minimisation and security should be resolved architecturally by relocating long-term and cross-context security analysis away from the device layer, treating terminal equipment as a point of intervention rather than a place of security intelligence, while doing broader security analytics to comply with Article 32 GDPR and the NIS 2 Directive.¹⁸⁷ Targeted legislative clarifications could explicitly limit the security exception to actively requested service functions, impose temporal limits on device-level access, and prohibit secondary use of data obtained under Article 88a(3), complemented by a recital clarifying that systemic and long-term cybersecurity monitoring belongs outside the terminal equipment layer.

A more structural solution would be to introduce an explicit legal basis for cybersecurity purposes within the GDPR, closely complementing Article 32 of the GDPR,¹⁸⁸ rather than relying on a device-level exception to accommodate broader security needs. Such a legal basis would allow controllers to process personal data for systemic, preventive, and long-term cybersecurity risk management, such as threat detection, anomaly analysis,¹⁸⁹ without stretching the logic of terminal equipment access. Crucially, this legal basis should be accompanied by clear limits: it should apply only where processing is strictly necessary to ensure the security of systems and services. In such an architecture, which is not currently provided for in the Proposal, Article 88a(3)(d) would remain a narrowly tailored endpoint-security exception.

¹⁸⁶ The example of security patching given in the Joint Opinion of the EDPB and EDPS is the reminder of this point; European Data Protection Board (EDPB) and European Data Protection Supervisor (EDPS), ‘Joint Opinion 2/2026 on the Proposal for a Regulation as Regards the Simplification of the Digital Legislative Framework (Digital Omnibus)’ (n 78).

¹⁸⁷ Article 21 of the NIS 2 Directive require certain entities to have cybersecurity risk management measures, which might include threat intelligence technologies. See for personal data processing for cybersecurity purposes under the NIS 2 Directive Eyup Kun, ‘Searching for the Appropriate Legal Basis for Personal Data Processing for Cybersecurity Purposes Under the NIS 2 Directive: Legal Obligation and/or Legitimate Interest?’ (2025) 56 Computer Law & Security Review 106098 <<https://doi.org/10.1016/j.clsr.2024.106098>>.

¹⁸⁸ See for personal data processing for cybersecurity requirements under the GDPR, Suzanne Nusselder, ‘Scrutinising the Interplay between Data Protection and Cybersecurity: A Paradox Shrouded Behind the “State-of-the-Art”’ (2025) 2 European Data Protection Law Review 145.

¹⁸⁹ See for insider threat detection technologies as a case study under the NIS 2 Directive, Kun (n 187).

3. AI Omnibus Proposal¹⁹⁰

3.1 Governance architecture of the AI Act

The AI Omnibus proposal introduces some crucial changes to the governance structure of the AI Act. Under the proposed new paragraph 1 of Article 75, first and second subparagraph, the AI Office shall be exclusively competent for the supervision and enforcement of the obligations under this Regulation in relation to AI systems that constitute or that are integrated into a designated very large online platform or very large online search engine within the meaning of Regulation (EU) 2022/2065¹⁹¹ (Digital Services Act, or DSA). As clarified by recital 15 of the legislative proposal,¹⁹² the EU legislator considered it appropriate to entrust the Commission with such powers to facilitate a coherent supervision and enforcement of the AI Act and the DSA. Moreover, recital 15 states that the Commission services responsible for the enforcement of the DSA may consult with the AI Office on risk assessments carried out under the AI Act, and that the competent services of the Commission under the DSA and the AI Act should coordinate their enforcement efforts, also with national authorities, to ensure that the principles of loyal cooperation, proportionality and non bis in idem are respected. Importantly, to exercise the new supervisory and enforcement tasks, the AI Office is conferred the powers of a market surveillance authority, as defined in the AI Act and in Regulation (EU) 2019/1020¹⁹³.

Problem 1: The AI Omnibus Proposal coordination of enforcement between the AI Act and the DSA is incomplete.

The proposed amendment would essentially make the AI Office the competent supervisory and enforcement authority for AI systems deployed in the media sector, with a consequent expansion of the AI Office's competences in relation to a significantly broad new range of sectorial application of AI systems. This expansion of the scope of the AI Office's competences can bring about both positive and negative changes. Starting with the positive, the change may bring more consistency in the overall governance architecture for very large online platforms or search engines (VLOPSEs). VLOPSEs are regulated at the EU level on the basis of the EU-wide nature of the systemic risks that they pose. Under the DSA, the European Commission is entrusted with the task to supervise and enforce the systemic risk management regime for these services in a manner that is consistent across the EU. AI systems can play an important role for the functioning of VLOPSEs and can consequently shape the systemic risks that they pose. For instance, AI systems can be used for the functioning of recommender systems and content moderation systems, both important potential sources of systemic risks, as well as avenues to mitigate systemic risks. Should AI systems be supervised by national market surveillance authorities, there would be significant risks of fragmented application of the AI Act, which could be detrimental to the EU-wide governance of VLOPSEs and the

¹⁹⁰ European Commission, 'Proposal for a Regulation of the European Parliament and of the Council Amending Regulations (EU) 2024/1689 and (EU) 2018/1139 as Regards the Simplification of the Implementation of Harmonised Rules on Artificial Intelligence (Digital Omnibus on AI)' (2025) COM(2025) 836 final-2025/0359 (COD) <<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52025PC0836>> accessed 26 January 2026.

¹⁹¹ Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance) (OJ L 277/1, 19/10/2022).

¹⁹² European Commission, 'Digital Omnibus on AI' (n 190).

¹⁹³ Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011 (Text with EEA relevance) (OJ L 169/1, 20/6/2019).

conduction of systemic risk management. While high-risk AI systems are unlikely to be used for the provision of VLOPSEs, there may be prohibited AI practices, in particular in relation to risks of manipulation, and limited-risk AI systems regulated under Article 50 of the AI Act.

Yet should this amendment to Article 75 be adopted, this would create further shortcomings in the resulting governance architecture, making the proposed change incomplete for two reasons.

First, as a part of a broader issue within Article 75, the AI Office would wear the two hats of market surveillance authority and AI Office and supervise AI systems' deployment in a context for which it may not have the requisite expertise. The task entails having to deal with different procedures, sets of powers and applicable legal framework. In order to supervise the application of the AI Act to AI systems used for the provisions of VLOPSEs, the AI Office would therefore need to develop expertise to understand VLOPSEs as a complex sociotechnical environment. For instance, to monitor the application of Article 5(1)(b) of the AI Act, the AI Office would need to understand how vulnerabilities can be exploited in the context of the provision of VLOPSEs, considering the nature and effects of the interaction between users and services, as well as how significant harm can be caused by the provision of VLOPSEs.

Second, such expansion of competences of the AI Office, coupled with the pre-existing tasks for the supervision of general-purpose AI models, increases the potential overlap of supervisory and enforcement activities with the services of the European Commission competent for supervision and enforcement under the DSA. While recital 15 of the legislative proposal does mention the need for cooperation and cooperation between the two services, the modalities are not fleshed out. Defining such modalities is a central nodal point to ensure consistency in the different streams of supervision and enforcement, especially exchange of information on the functioning of VLOPSEs and the risks they pose.

Recommendation

The modalities for cooperation and coordination between the AI Office and the Commission Directorate competent under the DSA should be regulated in more detail. Among others, it should be considered to require that, before the AI Office or the Commission Directorate competent under the DSA take a supervisory and enforcement action, they consult with each other, to ensure a consistent understanding of risks and a consistent enforcement policy. The exchange of information should be continuous and bi-directional, so that the evidence used to inform supervisory and enforcement action is as aligned as possible at all times. Without a continuous exchange of information. The modalities for cooperation and coordination between the AI Office and the Commission Directorate competent under the DSA should be regulated in more detail. Among others, it should be considered to require that, before the AI Office or the Commission Directorate competent under the DSA take a supervisory and enforcement action, they consult with each other, to ensure a consistent understanding of risks and a consistent enforcement policy. The exchange of information should be continuous and bi-directional, so that the evidence used to inform supervisory and enforcement action is as aligned as possible at all times. Without a continuous exchange of information, the effort of consistent EU-wide supervision and enforcement may be undermined.

Problem 2: The powers for the European Commission to define its own procedures via implementing act go beyond the limits for this legislative instrument.

Under the proposed new paragraph 1a of Article 75, the European Commission shall adopt an implementing act to define the enforcement powers and the procedures for the exercise of the powers set out in paragraph 1, regarding the supervision of AI systems with the same competences of market surveillance authority. Implementing acts can be adopted also to define the ability of the AI Office to impose penalties, such as fines or other administrative sanctions. The provision would essentially empower the Commission to define its own enforcement powers and the procedures governing their exercise. The definition of enforcement powers and related procedures would likely qualify as essential elements of a legislative act and go beyond just implementing provisions, which is the purpose of implementing acts. Such empowerment appears therefore to be contrary to the limitations, resulting from Article 290 and 291 of the TFEU, which mandate that the definition of essential elements of a legislative act is not delegated to the European Commission

Recommendation

The definition of the powers and related procedures to exercise them should be defined in the legislative act (the AI Act) and not delegated to the European Commission in order to respect the limits put for such instruments in EU primary law.

3.2 AI Literacy

The AI Omnibus Proposal introduces fundamental changes to the obligation on AI literacy as defined in Article 4 AI Act by changing the nature of the provision from an obligation on AI providers and deployers to an requirement for the European Commission and the Member States to take encouraging steps.¹⁹⁴ This change appears to be motivated by the assessment that a one-size-fits-all approach for AI literacy as currently implemented in Article 4 AI Act is not effective and hence unable to attain the goals initially set out with it. However, this does not necessarily justify the change in the nature of the provision. On the contrary, the diversity of AI systems and contexts strengthens the case for maintaining provider- and deployer-level obligations.

Problem 1: The AI Omnibus Proposal completely changes the nature of the AI literacy provision transforming it from a binding obligation to a policy instrument. This will not solve the issue of the one-size-fits-all approach that the amendment intends to solve.

One of the justifications laid down in the AI Omnibus Proposal for the revision of the AI literacy obligations, is to reduce administrative burdens for businesses.¹⁹⁵ The argument that AI literacy imposes disproportionate compliance costs, particularly on smaller enterprises, is unconvincing. Recital 5 of the Omnibus itself acknowledges AI literacy as a '**strategic priority**' but misses that the AI Act does not provide for **specific sanctions** for non-compliance with AI literacy obligation, thereby diverging from other AIA requirements. Moreover, a growing number of **free or low-cost AI literacy programmes**,¹⁹⁶ initiated by Member States, public bodies, and private actors, substantially weakens claims that AI literacy entails significant financial burden and begs for justification.

¹⁹⁴ European Commission, 'Digital Omnibus on AI' (n 190) 12–13, para 5.

¹⁹⁵ *ibid* 6 and 12.

¹⁹⁶ See for example the non-exhaustive list for AI literacy initiatives, Tânia Figueiredo, 'AI Literacy Programs in Europe – Supporting Article 4 of the EU AI Act | EU Artificial Intelligence Act' (23 May 2025) <<https://artificialintelligenceact.eu/ai-literacy-programs/>> accessed 6 March 2026.

At the same time, shifting responsibility for AI literacy guidance as foreseen in the proposal, risks creating an **unworkable task for the European Commission and Member States**, which would require them to account for the technical and contextual specificities of a wide variety of AI systems developed and deployed across sectors. This increases the likelihood of **overly generic, context-insensitive guidance**, disconnecting AI literacy efforts from the realities of AI development and use and, paradoxically, reintroducing the very **one-size-fits-all approach** the proposed revision seeks to avoid.

Additionally, the article as it stands now in the AI Act already allows for context appropriate implementation referring to technical knowledge, experience, education, and training.¹⁹⁷ Hence the problem does not seem to be the very existence of an obligation, but rather the need for more guidance/flexible execution. This is something that providers and deployers themselves are best placed to deliver. This leads to second point below.

Problem 2: The proposed change to AI literacy fails to take account of the system-specific knowledge that is only available to the providers and deployers of AI systems.

Providers and deployers are in the unique position to provide the relevant and operational literacy to staff in regard to the specific AI system at hand. This is also explicitly stated in the preamble of the current AI Act.¹⁹⁸ The European Commission and Member States may be better positioned to provide for the more general and societal aspects of the implementation of AI by cooperating with organizations and educational institutions.¹⁹⁹ However, one cannot be replaced by the other. AI literacy is most effective when it is embedded in routines and daily workings of systems, allowing for continuous adaptation to new evolutions of these AI systems.²⁰⁰ This notion is reflected in the preparatory versions of the current AI Act.²⁰¹ Hence, removing providers and deployers from the obligation waters down both the quality and specificity of AI literacy.

Moreover, AI literacy, and the system-specific knowledge possessed by the providers and deployers that corresponds to this, has a significant role by **enabling** compliance with the AI Act and is instrumental in achieving its core objectives of mitigating risks to **health, safety, and fundamental rights of individuals**.²⁰² In particular, **meaningful human oversight** presupposes a sufficiently high level of AI literacy among those tasked with supervising AI systems, as oversight without understanding system capabilities, limitations, and risks is ineffective. Accordingly, **irrespective of any revisions to Article 4**, AI literacy remains an

¹⁹⁷ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (OJ L, 12/7/2024) art 4 (AI Literacy).

¹⁹⁸ *ibid* recital 91.

¹⁹⁹ UNESCO, 'Recommendation on the Ethics of Artificial Intelligence (23 November 2021) SHS/BIO/PI/2021/1' 16-17. Policy Area 8 <<https://unesdoc.unesco.org/ark:/48223/pf0000381137>> accessed 6 March 2026.

²⁰⁰ Brando Benifei and Dragoş Tudorache, 'Report on the Proposal for a Regulation of the European Parliament and of the Council on Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts' (European Parliament, Committee on the Internal Market and Consumer Protection, Committee on Civil Liberties, Justice and Home Affairs 2023) P9_A(2023)0188_EN Amendments 28, 120, 214 <[https://www.europarl.europa.eu/RegData/seance_pleniere/textes_depotes/rapports/2023/0188/P9_A\(2023\)0188_EN.pdf](https://www.europarl.europa.eu/RegData/seance_pleniere/textes_depotes/rapports/2023/0188/P9_A(2023)0188_EN.pdf)> accessed 6 March 2026.

²⁰¹ *ibid*.

²⁰² European Data Protection Board (EDPB) and European Data Protection Supervisor (EDPS), 'Joint Opinion 2/2026 on the Proposal for a Regulation as Regards the Simplification of the Digital Legislative Framework (Digital Omnibus)' (n 78) para 43.

indispensable intermediary condition for the practical application of the AI Act's obligations rather than an optional requirement or encouragement.²⁰³

Problem 3: The proposed changes to Article 4 undermine the level of protection of safety, health, and fundamental rights the AI Act is aiming for.

AI Literacy has broader social, ethical, and cultural dimensions. Hence, any revision concerning AI literacy obligations (in)directly affects the level of protection of safety, health, and fundamental rights, of the AIA (recital/article).

The AI Omnibus proposal asserts that the revisions do not affect fundamental rights because they 'do not affect the scope of the regulated AI systems or the substantive requirements applicable to those systems' (p. 6). This claim is incomplete. While the formal scope may remain unchanged, among other revisions, **weakening AI literacy obligations has material implications for the protection of fundamental rights**, as it reduces the capacity of deployers and human overseers to identify, prevent, and respond to rights-infringing AI practices. In this sense, changes to AI literacy obligations indirectly, but significantly, affect the effective protection of individuals under the AI Act.

Furthermore, as asserted in the current AI Act recitals and scholarly commentary: AI literacy is not limited to the mere technical understanding or risk awareness of AI systems. It has a plethora of aspects, such as ethical considerations, societal impacts, cultural/organizational effects, and more.²⁰⁴ Article 4 as it stands now already received criticism for its narrow character due to disregarding these other dimensions.²⁰⁵ AI literacy is not just a tick-the-box obligation but an ongoing process involving various factors.²⁰⁶ Hence if the obligation is weakened even further, these broader dimensions are even more removed from AI literacy today and will leave it completely up to the goodwill of providers and deployers to consider the dimensions of AI systems beyond technical and risk education. This is also echoed by the EDPB and EDPS, in their most recent joint statement, affirming that AI literacy promotes understanding of AI and awareness of its ethical and social risks and benefits, enabling informed decision-making and supporting compliance with AI rules and the protection of fundamental rights. Moreover, reducing the AI literacy obligation to a mere duty to encourage would significantly weaken its effectiveness and undermine its objective.²⁰⁷

Recommendation

Instead of weakening the AI literacy obligation, we propose that the European Commission strengthens it by introducing a two-Layered AI Literacy Obligation. The first layer remains as is currently the case addressed to deployers and providers of AI systems. This ensures

²⁰³ *ibid.*

²⁰⁴ Elora Fernandes, Wayne Holmes and Sopio Zhgenti, 'Article 4 AI Literacy' in Ceyhun Necati Pehlivan, Nikolaus Forgó and Peggy Valcke (eds), *The EU Artificial Intelligence (AI) Act - A Commentary* (Wolters Kluwer 2024) 86–104; AI Act recitals 60, 91, 165; Gabriele Biagini, 'Towards an AI-Literate Future: A Systematic Literature Review Exploring Education, Ethics, and Applications' (2025) 35 *International Journal of Artificial Intelligence in Education* 2616, 2639 <<https://doi.org/10.1007/s40593-025-00466-w>>.

²⁰⁵ Fernandes, Holmes and Zhgenti (n 204) 95-96 Defining AI Literacy.

²⁰⁶ AI Act art 3(56) (AI Literacy); Fernandes, Holmes and Zhgenti (n 204) 97.

²⁰⁷ European Data Protection Board (EDPB) and European Data Protection Supervisor (EDPS), 'Joint Opinion 1/2026 on the Proposal for a Regulation as Regards the Simplification of the Implementation of Harmonised Rules on Artificial Intelligence (Digital Omnibus on AI)' (2026) 13–14 <https://www.edpb.europa.eu/system/files/2026-01/edpb_edps_jointopinion_202601_proposal_ai-omnibus_en.pdf> accessed 6 March 2026.

sufficient knowledge for the sector specific and more technical aspects of AI Literacy. We therefore would go back to the original text of Article 4 AI Act.

In the second layer, the proposal could introduce an addition to Article 4, which foresees a role for the European Commission, the AI Office, Market Surveillance Authorities, and Member States, to take into account the broader (legal, ethical, societal, cultural) implications of the widespread use of AI systems. This is also reflected in paragraph 46 of the recent joint opinion by the EDPS and EDPB, as well as in the study recently commissioned by the European Parliament's Committee on the Internal Market and Consumer Protection (IMCO).²⁰⁸

²⁰⁸ *ibid* 14; Goda Skiotytė and Audronė Sadauskaitė, 'A Digital Omnibus: Identifying Interlinks and Possible Overlaps Between Different Legal Acts in the Field of Digital Legislation to Streamline Tech Rules' (European Parliament 2026) Study requested by the IMCO committee PE 772.641 <[https://www.europarl.europa.eu/RegData/etudes/STUD/2026/772641/ECTI_STU\(2026\)772641_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2026/772641/ECTI_STU(2026)772641_EN.pdf)> accessed 6 March 2026.

4. Other changes proposed in the Digital Omnibus Proposal

4.1 The new pro-industry approach towards data legislation

Problem 1: The amendments proposed to the Data Legislation ('Data Acquis' as referred to by the EU Commission) through the creation of a single Data Act are marked as 'targeted and technical in their nature',²⁰⁹ but a comprehensive reading of the Digital Omnibus Proposal points towards a reinforcement of business interests vs. a lowering of protection of non-business related rights and prerogatives

The Digital Omnibus Proposal aims at making the Data Act – the key piece of data market-oriented legislation – the main legal instrument for data regulation, including the governance of public data. This suggests that the legislature intends to prioritise a pro-industry and pro-market approach to data regulation,²¹⁰ still heavily regulated in favour of business actors, to the detriment of democratic, collective and public interest oriented governance of data.²¹¹ This overarching trait of the proposal is evident in the fundamental rights section of the Explanatory Memorandum, whereby the promotion of the right to conduct a business in the Union is prominent over the consideration of the other fundamental rights.²¹²

This pro-industry legislative aim goes beyond mere technical amendments, as specifically substantiated by more protective regimes for businesses and private interests, characterizing all the amendments to the Data Act and to the Data Governance Act. Namely, (i) the added emphasis on trade secret protection based on a risk assessment evaluation entrusted to the data holder, to justify the refusal to share IoT-data with third countries (*see section 4.5 below*); (ii) the stricter condition of 'public emergency' instead of 'exceptional need' to make available data to public entities for public interest; (iii) the stricter conditions for cloud switching; and (iv) the facilitated regime for data intermediation services and data altruism organizations. These amendments considered cumulatively move in the direction of reinforcing secrecy, confidentiality and business interests against publicness and accessibility.

A clear manifestation of this pro-market trend is noted in the 'principles governing charging for open government data' set out by the Article 32q of the Digital Omnibus Proposal. It states that public sector bodies can ask for 'higher charges' 'proportionate and based on objective criteria' for the re-use of open government data by very large enterprises.²¹³ However, the proposal and the accompanying document do not clarify how the possibility to set out a higher fee – that large enterprises will be easily able to pay – as the only additional condition for their re-use of open government data, would foster a fair competition and relatedly being beneficial to society as a whole.²¹⁴

By contrast, when it comes to safeguarding the individual and the collectives in the face of the use of personal data relating to them, the amendments to the GDPR move in the opposite

²⁰⁹ European Commission, 'Digital Omnibus' (n 30) 14; European Commission, 'SWF Digital Omnibus' (n 27) 4.

²¹⁰ As pointed out by Barbara Lazarotto, 'The Data Omnibus: The Good, the Bad, and The Ugly Behind the DGA and Data Act Rewrite' (*MediaLaws*, 19 December 2025) <<https://www.medialaws.eu/the-data-omnibus-the-good-the-bad-and-the-ugly-behind-the-dga-and-data-act-rewrite/>> accessed 6 March 2026.

²¹¹ A similar observation has been raised by Skiotytė and Sadauskaitė (n 208) 45–46.

²¹² European Commission, 'Digital Omnibus' (n 30) 15.

²¹³ *ibid* 42.

²¹⁴ European Commission, 'SWF Digital Omnibus' (n 27) 13–16.

direction of lowering the level of protection, as notably by allowing the reliance on the legal basis of legitimate interest for AI development and operation (*see sections 2.3 and 2.7*).

The amendments proposed, marked as technical in nature, are in fact substantial and the result of specific political choices, against a wealth of studies on the shortcomings of adopting a pro-industry and/or pro-market approach to data regulation and on viable alternatives.²¹⁵

Problem 2: The Digital Omnibus Proposal suffers from methodological and legislative opacity.

Beyond its substantive reorientation of EU data law, the Digital Omnibus Proposal raises concerns as to its legislative technique, i.e. simultaneously incorporating existing provisions into the Data Act while materially amending them. By introducing new provisions in the Data Act that formally correspond to existing articles in other instruments yet diverge from them in substance or omit key elements without signalling these amendments explicitly, the proposal makes it difficult for legislators, practitioners and affected stakeholders to ascertain the actual scope and effects of the changes introduced. This results in a significant loss of transparency and legal certainty, which runs directly against the simplification objective allegedly pursued by the proposal.

The correlation table in Annex I does not suffice to tackle this issue. This is illustrated by the (former) article(s) on the tasks of the European Data Innovation Board. While the correlation table suggests a formal continuity between Article 30 of the DGA and the new Article 42 of the Data Act, closer scrutiny reveals that some of the tasks explicitly mentioned in the current version have not been retained by the new provision included in the proposal (see the discussion in section 4.7.2 of this document). This substantive omission is largely obscured by the technique of incorporation and would have been far more visible had it been introduced through a direct amendment to the DGA. As such, the proposed approach contributes to normative ambiguity and undermines informed democratic and legal scrutiny of the proposal's real implications.

Recommendations

We ask the European Commission to be explicit about the substantial and political nature of the amendments proposed and their objectives. The substantial nature of the amendments needs to be clearly stated and motivated in relation to the objectives pursued. The legitimacy of the proposal would be safeguarded: 1) by providing evidences that pursuing a pro-industry and pro-market approach to data regulation will be able to deliver on the fair competition and broader societal objectives; 2) by evaluating alternatives or complementary measures through a full impact assessment; and 3) by conducting a proper fundamental rights evaluation, where the freedom to conduct business is appropriately balanced against competing rights and interests, including not only the rights to privacy and data protection, but also the freedom of thought, the freedom of arts and sciences, the right not to be discriminated against as well as environmental and consumer protection, by way of examples.

We also urge the European Commission to adopt a more transparent and orthodox legislative technique when introducing substantive changes to existing data law instruments. In

²¹⁵ Ex multis, Charlotte Duceing, 'Data as a Contested Commodity' (2024) 24 Global Jurist 277 <<https://doi.org/10.1515/gj-2024-0065>>; Nadya Purtova and Gijs van Maanen, 'Data as an Economic Good, Data as a Commons, and Data Governance' (2023) 16 Law, Innovation and Technology 1 <<https://doi.org/10.1080/17579961.2023.2265270>>; Tommaso Fia and Gijs van Maanen, 'Through Thick and Thin: Data Commons, Community and the Struggle for Collective Data Governance' (2025) 2025 Technology and Regulation 114 <<https://doi.org/10.71265/tk2x3d39>>.

particular, material deletions, reformulations or reallocations of competences should be explicitly set out as direct amendments to the existing legislation (at least in a first step or in preparatory works), rather than being implicitly affected through incorporation into a new instrument. Such an approach would enhance clarity, legal certainty and democratic accountability, and would be more consistent with the requirements of the EU's multi-layered legal order.

4.2 Implications of merging the Open Data Directive, the Data Governance Act into the Data Act

Problem 1: The proposed changes brought by the Digital Omnibus Package²¹⁶ focus on the re-use of data for commercial purposes, overlooking non-commercial goals.

Part of the Digital Omnibus Proposal includes a merging of (parts of) three different legislative instruments (the Open Data Directive (ODD), the Data Governance Act (DGA), and the Data Act (DA)) into a new 'Data Act'. Yet, incorporating the ODD into the new Data Act left behind key elements and considerations about data's potential for democratic, societal, and public interest goals.²¹⁷ The potential of data encompasses using data for both commercial and non-commercial purposes. Goals beyond economic profit entail democratic goals, such as transparency, societal engagement and oversight, and memory preservation, and other public interest purposes, including fundamental research, accountability, knowledge sharing and scientific research, among others. In other words, recognition of non-commercial purposes is closely connected with achieving public interest goals.

Data's role in achieving these objectives has been recognised, at least in the legal text, in various EU legal instruments, including the DGA, the DA, and, more evidently, the ODD. As an example, definitions of data re-use provided by both the DGA and the ODD include non-commercial purposes as one of the legitimate justifications for re-use. In the same lines, the European Data Strategy highlighted the potential of privately held data for the public sector's re-use for the public interest and the importance of connecting and facilitating data sharing or re-use between public and private entities. However, public interest goals are not further developed or detailed in any of the legal instruments.

Revisiting the rules on data re-use via the Digital Omnibus Proposal could have served as an opportunity to implement specific rules to guarantee that the public interest in data use and re-use is fully explored. Instead, the societal interests are shadowed by commercial objectives, especially AI development. For instance, even though the new proposed Data Act, resulting from the merger of the ODD, DGA and the current DA, does adopt the concept of re-use which includes non-commercial purposes, this is solely connected to documents held by public sector bodies or public undertakings, leaving behind the recognised potential of private-held data for societal goals. Principles closely related to societal and democratic ideas of open data are left behind or randomly mentioned in the legal text. The principle of 'as open as possible, as closed as necessary', for example, is loosely brought in Article 32t, related to research data, without any further details.

At the same time, the newly proposed legal text abandons the term 'open data', which even historically can be connected to societal and democratic goals of data use. Also, non-

²¹⁶ European Commission, 'Digital Omnibus' (n 30).

²¹⁷ Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (recast) 2019 (OJ L 172/56, 20/6/2019).

commercial purposes or public interest(s) are not mentioned in the introductory text to the Digital Omnibus Proposal, and neither are they listed as goals in the call for evidence. At the same time, the Data Union Strategy mentions “public interest” only twice in its text, while ‘AI development’ is mentioned at least 14 times.²¹⁸ These choices lead to fewer discussions on solutions related to societal and democratic goals, missing the opportunity to even highlight how AI development can be connected to these purposes.

On the other hand, Section 2 of the new Data Act, which provides a more detailed framework for the re-use of open government data, is welcomed and should also be understood as an instrument for the public interest. The same goes for the non-discrimination principle, adopted in Article 32j of the proposed Data Act and reinforced throughout the text. Choosing not to use the term ‘open data’ should not diminish the democratic ideals behind open government data and its re-use. On the same lines, the merger of norms proposed by the Digital Omnibus Proposal and the choice of maintaining ‘Data Act’ as the terminology for the new instrument should not lead to a disappearance of public interest goals, especially without exploring the benefits of private-held data for the common good. More emphasis should be placed on that.

Recommendations

The objectives of the current ODD and DGA (the part on open sector data) and the Data Act are very different. To preserve the underlying ideas of the ODD on open data and re-use of public sector data for the public interest, we suggest to not merge the three instruments. Instead, only the ODD should be merged with the relevant sections on re-use of public sector data of the DGA. The other sections of the DGA (data intermediaries, data altruism, governance) could then be merged with the current Data Act. This preserves each act’s legislative purpose and avoids interpretative conflicts based on unclear legislative intent behind certain provisions.

If the European Commission insists on going ahead with the merger of all three instruments, we strongly suggest that such a merger should: incorporate more provisions and clarifications on non-commercial purposes and public interest uses of data, developing and emphasising the new Data Act’s role in opening data for these objectives. This could be done via adding specific recitals on the matter, and by offering more legal certainty to undefined concepts and principles, especially of the ‘as open as possible, as closed as necessary’ principle. The European Commission should also foresee instruments allowing for the full exploration of privately held data for the public interest, alongside the necessary safeguards, within the newly formed Data Act. Finally, the new Data Act should clarify that non-commercial purposes, including societal participation and oversight, are central objectives for exploring the full potential of data. Non-discrimination should be understood as a guiding principle for allowing the data re-use, for different purposes, including non-commercial ones.

Problem 2: None of the proposed changes provides enough clarification on the difference between data access and data re-use, which further complicates the distinction of both in the data lifecycle.

²¹⁸ See European Commission, ‘Communication from the Commission to the European Parliament and the Council Data Union Strategy Unlocking Data for AI’ (2025) COM(2025) 835 final, 19/11/2025 (Data Union Strategy). The term ‘AI’ is mentioned more than 100 times.

Allowing data re-use is considered a key element by the EU's recent policies to develop the economy and fully explore data's potential. This objective was part of the different norms now merged into the proposed new Data Act and is a central element to the changes brought by the Digital Omnibus Proposal. The proposal thereby equates data re-use with data access, which is however a different step in the data lifecycle as confirmed in the distinct definitions of the ODD. The CJEU has confirmed this distinction in the *HP – Hrvatska pošta d.d. - v. Povjerenik za informiranje* case, where it evaluated a disagreement on the application of the ODD and, in its decision, differentiated data access from data re-use²¹⁹. This confirms that both acts are distinct, even though neither the Court nor the proposed amendments clarify what this would entail in practice. Data access however might in some situations, e.g. when motivated by a strong public interest, be possible where data re-use is not. Without clarity on what each term means and how they relate to each other, there is a risk that public authorities opt for the most protective approach, which undermines both access and re-use.

This problem is worsened by the proposed merger of the legislative frameworks. By incorporating (former) DGA provisions into the (newly merged) Data Act, the Digital Omnibus Proposal copies the definition of 'data access' as per the DGA. This definition of data access equates access with data use, contradicting the understanding of the CJEU outlined above.²²⁰ Moreover, the ODD explicitly states that, in mandating and governance data re-use, it builds on and is without prejudice to data access²²¹ with respect to public sector data, with due regard to the competences of Member States. Data re-use is defined as the *use* of some (namely public sector) data.²²²

Recommendations

As noted in the previous recommendation section, we suggest to not merge the ODD, DGA and the DA, due to their diverging objectives, but in this case also their heterogeneous definitions.

If a merger goes ahead, we propose to clarify in the legal text and throughout specific recitals, how the different concepts of data access, openness, and data (re-)use can co-exist and how each obligation connects to the framework established by the new Regulation. A way forward could be to distinguish *practical* or technical operations from *legal* notions (i.e. pointing to rights on or in connection to data), informed by the language of property law.²²³

4.3 The unsolved issues with institutionalised data sharing

The problem: While the Digital Omnibus Proposal recognizes that an actual market for data intermediary services and data altruism organizations is (still) not in place²²⁴ and specifically that expectations for the establishment of such market have not been met,²²⁵ the proposal makes negligible amendments to the legal regime of these entities.

The Explanatory Memorandum of the Digital Omnibus Proposal states that the suggested interventions on the DGA would serve 'to boost the attractiveness' of data altruism and data

²¹⁹ *HP - Hrvatska pošta dd v Povjerenik za informiranje* [2024] ECJ Case C-336/23.

²²⁰ Data Governance Act art 2(13); and European Commission, 'Digital Omnibus' (n 30) art 1(2).

²²¹ Open Data Directive art 1(3).

²²² *ibid* 2(11).

²²³ Duccing, *Data Commodification and the Law: Navigating Data Markets and Data Protection* (n 56) 169–173.

²²⁴ European Commission, 'SWF Digital Omnibus' (n 27); European Commission, 'Digital Omnibus' (n 30).

²²⁵ European Commission, 'SWF Digital Omnibus' (n 27) 10.

intermediation services as data sharing mechanisms,²²⁶ by making their obligations ‘more flexible for this market to grow’.²²⁷

The adjustments proposed concern: (i) the regime for operating data intermediation services, which is made voluntary in the sense that it grants a label, rather than being mandatory as of now (ii) the requirement to provide data intermediation services through a separate legal entity, which is converted into a mere functional separation; (iii) a general lightening of the obligations of data intermediation service providers and data altruism organizations, the latter specifically with regard to transparency and reporting.

According to the European Commission, the lowering of the administrative burden and of the related costs will stimulate this ‘emerging market’ and, ‘implicitly, value creation through the reuse of data’.²²⁸ However, the proposal does not question data altruisms and data intermediation services as overall mechanisms to enhance data sharing and boost ‘value creation’, despite acknowledging their very limited uptake.²²⁹ In particular, it is not clear how the voluntary regime for data intermediation services providers or a reduced administrative burden for data altruism organization would as such boost ‘the market’, as the benefits of such mechanisms are not explained and articulated. Specifically, the European Commission does not consider at all the possibility that lowering the administrative burden to put in place data intermediation services and data altruism would, on the contrary, simply lead to the defeat of this ‘market’, as it already happened with voluntary mechanisms in other domains.²³⁰

In particular, the European Commission did not consider the more fundamental critiques to the legal regime of data intermediaries as per the DGA and especially the conceptual incompatibility of the DGA references to and use of GDPR notions with both the letter and spirit of the GDPR,²³¹ which is not addressed by turning a mandatory regime into a voluntary one. Furthermore, the European Commission does not draw the consequences of empirical economic research showing that data sharing does overwhelmingly occur in the context of governance mechanisms other than data markets.²³²

Recommendations

We recommend the European Commission to acknowledge the very limited uptake of data sharing mechanisms provided for by the DGA, as is to a certain extent done in the Digital Omnibus Proposal. This should in turn prompt a broader evaluation of the means put in place to enhance data sharing and of the targeted objectives, rather than a slight modification of the current regime. The European Commission should also use the opportunity of a recast of the DGA as a chance to ensure compatibility with the GDPR.

²²⁶ European Commission, ‘Digital Omnibus’ (n 30) 4.

²²⁷ *ibid* 16.

²²⁸ European Commission, ‘SWF Digital Omnibus’ (n 27) 11.

²²⁹ *ibid* 10, 17.

²³⁰ As for instance, it happened in the case of the voluntary registration to enable cross-border digital identification under eIDAS Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257/73 28/8/2014).

²³¹ Ducuing, *Data Commodification and the Law: Navigating Data Markets and Data Protection* (n 56).

²³² For a recent study, see for example Lucas Eustache, Eric Brousseau and Joëlle Toledano, ‘The Economics of Data-Sharing: An Empirical Investigation of Data Sharing Ecosystems’ [2025] ICIS 2025 Proceedings <https://aisel.aisnet.org/icis2025/sharing_econ/sharing_econ/6>.

We urge the European Commission to gather more input on the needs for data re-use. Acquiring inputs from business actors is considerable and relevant for a policy and legislative choice to be sustained, but it is not the only factor that determines the success of the solution. In this sense, the Proposal should (i) identify a clear articulated and substantiated need(s) for which the (re)use of data would lead to ‘value creation’²³³ (which value and for whom?); (ii) enable the acquisition of inputs from academia, civil society and smaller businesses on the identification of such needs; (iii) before putting forward new rules, evaluate the existing legal framework, not limited to data regulation, but comprising competition law and the EU consumer acquis and their enforcement in tackling the identified needs; and (iv) elaborate and put forward new regulatory solutions only after a full impact assessment.

4.4 Access by public authorities to privately-held data on the basis of an exceptional need

Under Chapter V of the (current) Data Act (DA), making data available to public authorities on the basis of an **exceptional need** (Article 14 DA) entails two situations, on the basis of Article 15 DA:

- a) Response to a public emergency, whereby that data could not have been obtained otherwise (Article 15(1)(a) DA), **OR**
- b) Fulfilment of tasks in the public interest (e.g. production of official statistics or the mitigation of or recovery from a public emergency) (Article 15(1)(b) DA).

The Digital Omnibus Proposal substantially amends the said Chapter by **deleting both Articles 14 and 15** (instead of being replaced) and **inserting a new Article 15a**. According to its provision, public authorities can ask for data to be made available by private actors when there is an exceptional need which necessitates the use of data in the public interest, necessary for responding to, mitigating, or supporting the recovery from a public emergency. The following problems can be thereto identified:

Problem 1: The Digital Omnibus Proposal consolidates the previous acquis (exceptional need *and* public emergency) despite the aim of narrowing down the scope of Article 15 DA.

The rationale behind this amendment is/was to clarify the – admittedly – broad margin of manoeuvre for public authorities to request data under Article 15(1)(b) DA. The objective of the European Commission was thus, as per recital 15 of the Digital Omnibus Proposal, to ‘narrow the scope of Chapter V from ‘exceptional needs’ only to ‘public emergencies’’. **However, such phrasing is not consistent with the wording of Article 15a.** More specifically, Article 15a narrows down the situations of ‘exceptional need’ from two (2) to one (1), by essentially integrating a part of Article 15(1)(b) (i.e. that on mitigation or recovery from a public emergency) to Article 15(1)(a) (i.e. response to a public emergency). **It does not eliminate the concept of exceptional need, which is still very much present in Article 15a.** Consequently, instead of strictly limiting Chapter V to public emergency response, the proposal effectively consolidates the previously distinct situations without clearly redefining their scope.

Recommendation

We urge the European Commission to clarify the relationship between the concepts of ‘exceptional need’ and ‘public emergency’. If the policy objective is indeed to restrict the mechanism to public emergency situations, the text of Article 15a should explicitly reflect this

²³³ European Commission, ‘SWF Digital Omnibus’ (n 27) 11. *ibid.*

by either **removing the notion of ‘exceptional need’** or **clearly defining it** as being limited to circumstances directly linked to a recognised public emergency.

Problem 2: The proposed changes fails to address longstanding challenge of divergent national interpretations of ‘public emergency’.

Another concern – which was already identified under the (current) Data Act regime – is related to the different national approaches to the notion of ‘public emergency’, and the inconsistencies resulting therefrom. The high degree of variation between Member States and their engagement with the concept of public emergency (in terms of defining it, having produced relevant legislation on and defined respective processes in declaring it) creates significant uncertainty,²³⁴ which has not been recognised nor addressed by the European Commission in the Digital Omnibus Proposal.

Moreover, in its recently published FAQ on the Data Act, the European Commission does not shed much light on this impasse:

What qualifies as ‘mitigation of or recovery from’ a public emergency?

*The Data Act does not clarify these concepts, but Article 15 clearly distinguishes them from ‘public emergency response’ (Article 15(1)(a)), which suggests that they are distinct from the actual occurrence of a public emergency, in particular in terms of timing. The factors to be considered when identifying an activity as ‘mitigation or recovery from a public emergency’ are likely to be laid down in national law, because mitigation or recovery from a public emergency must be designated as a “specific task carried out in the public interest, that has been explicitly provided for by law” in order to be relevant for Chapter V requests.*²³⁵

What is striking in that regard is the fact that (in spite of this FAQ having been published in late January 2026, hence almost two months after the publication of the Digital Omnibus Proposal in late November 2025) there is no reference to the situation likely to be created by the ‘new’ DA, whereby the two previously distinct situations – the response to, on the one hand, and the mitigation and recovery from a public emergency, on the other – appear to be merged.

Recommendation

We recommend the European Commission to provide interpretative clarifications vis-à-vis the different stages of ‘public emergency’ (i.e. response, mitigation and recovery). These phases have distinct operational timelines and policy objectives, and conflating them within a single provision risks creating interpretative difficulties. **A minimum harmonised definition of ‘public emergency’ should be introduced**, and/or at least some common criteria/indicators for their identification be established.

Problem 3: The proposed change leads to further interpretative complications from the addition of ‘public interest’ in relation to emergency response.

²³⁴ Heinrich Amadeus Wolff, Stefan Brink and Antje von Ungern-Sternberg (eds), ‘Artikel 15 Außergewöhnliche Notwendigkeit Der Datennutzung’ *BeckOK Datenschutzrecht: DS-GVO, BDSG, Grundlagen, Bereichsspezifischer Datenschutz - Kommentar* (51st edn, CH BECK 2025).

²³⁵ European Commission, ‘FAQs - Data Act’ (2026) <file:///C:/Users/u0170521/Downloads/FAQs_Data_Act_y6CNIhysdFESA1wcWyAFSnkao_108144.pdf>. *ibid.*

If the notion of ‘public interest’ previously concerned only the mitigation and recovery from a public emergency, it is now expanded to cover the response to such emergency. The notion of ‘public interest’ is particularly relevant here because, as showcased above, it has to be assessed in light of national legislation. This was previously not the case: there was no reference to public interest insofar the response to a public emergency was concerned. **This adds an additional layer of complexity in ensuring that all these conditions are met (public emergency and public interest cumulatively), thereby making access by public authorities to privately-held data ever rarer.**²³⁶

Recommendation

We propose to European Commission to provide that the declaration of a public emergency itself satisfies the public interest requirement, or limit ‘public interest’ to mitigation and recovery tasks, where longer-term policy measures are involved.

4.5 Competent authorities and enforcement under the Data Act

Problem: The Digital Omnibus Proposal further complicates the enforcement structure of the Data Act rather than simplifying it.

Within the Digital Omnibus Proposal, there is a sudden appearance of the need for competent authorities under the Data Act to be ‘set up’ in a manner that ensures **independence of competent authorities from the data intermediation service providers and data altruism organisations** (Article 32b(2)). This provision is overlapping with the already existing one of Article 37(8), which is already foreseeing the obligation for competent authorities to remain impartial and ‘free from any external influence, whether direct or indirect, and not to seek or take instructions for individual cases from any other public authority or any private party’. Neither the Annex²³⁷ nor the SWD²³⁸ accompanying the Digital Omnibus Proposal make any reference to the need for this separate/specific addition and/or any possible reasons justifying it.

The use of the phrasal verb ‘set-up’ also implies that the competent authority that is responsible for the registration of data intermediation service providers and altruism organisations needs to be new authority and not an already existing one. **This is in contradiction with Article 37(1)** which leaves a large margin of manoeuvre to the Member States to choose whether the public authorities they designate as competent are (a) newly established or (b) pre-existent.

Along the same lines, Article 32z speaks of ‘competent bodies’ which Member States can either establish or rely on existing ones for the purposes of complying with the provisions of Section 3 on re-use of certain categories of protected publicly held data. This designation shall

²³⁶ See also European Data Protection Board (EDPB) and European Data Protection Supervisor (EDPS), ‘Opinion 2/2026 on the Proposal for a Regulation as Regards the Simplification of the Digital Legislative Framework (Digital Omnibus)’ (2026) 35 <https://www.edpb.europa.eu/system/files/2026-02/edpb_edps_jointopinion_202602_digitalomnibus_en.pdf, where the EDPB and EDPS asks for clarifications on the difference between ‘responding’ and ‘mitigating or supporting’ the recovery from a public emergency.

²³⁷ European Commission, ‘Annexes to the Proposal for a Regulation Amending Regulations (EU) 2016/1679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854, (EU) 2024/1689 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as Regards the Simplification of the Digital Legislative Framework, and Repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus) (1/2)’ (2025) COM(2025) 837 final. *ibid*.

²³⁸ European Commission, ‘SWF Digital Omnibus’ (n 27). *ibid*.

be made in accordance with Article 37, however **the relationship between the concept of ‘competent authority’ and ‘competent body’ is not clarified.**²³⁹

Following from the above, **the interaction between Article 37 as an ‘umbrella’ provision, and Articles 32b and 32z remains unclear.** In light of the already identified degree of complexity of the enforcement landscape under the current regime,²⁴⁰ an attempt to merge the tasks of competent authorities of multiple legislations at once without ensuring transparency and clarity would further increase this complexity.

EU data legislation (including the Data Act and the DGA) is characterized by the key role assigned to administrative enforcement agencies (irrespective of how they are named), leading to heightened complexity. Especially, such agencies shall engage in various types of (inter-sectoral, cross-border, across various branches of the law, etc.) cooperation, which may affect their swiftness, efficiency and may lead to various types of legal uncertainties and fragmentation. While such issues are archetypical targets for any simplification endeavour, they are not addressed by the Digital Omnibus Proposal.

Recommendation

It is recommended that the DOP considers simplifying the administrative enforcement of EU data legislation. Several avenues have already been put forward, such as: (i.) harmonizing the rules for cooperation in EU legislation; (ii.) narrowing down the scope of the powers of administrative enforcement agencies, for example by enabling private actors such as data intermediaries to play a role in facilitating mandatory data sharing; (iii.) reducing the overlaps between the role assigned to administrative enforcement agencies and this of other bodies (such as dispute resolution bodies or the EDIP); (iv.) reducing the legal scope of the competence of administrative enforcement, for example by leaving out private law regimes such as this of B2B data contractual clauses. Instead and having due regard to the institutional autonomy of member States, specialized courts could be entrusted with data legislation-related enforcement.

4.6 Changes to the cybersecurity framework

The problem: The newly introduced single-entry point for incident and breach reporting is not merely a neutral transmission channel. It is a digital system, managed by ENISA, that stores reports, which may contain personal data. Yet the proposed changes provide only little guidance on how to square cybersecurity and GDPR requirements, in particular in terms of accountability.

The introduction of a single-entry point for incident and breach reporting under the Digital Omnibus Proposal represents a significant procedural reconfiguration of EU cybersecurity breach reporting. Article 23a of the NIS 2 Directive is intended to streamline reporting across multiple legal instruments, including the GDPR, NIS 2, DORA,²⁴¹ eIDAS,²⁴² and the CER

²³⁹ To be noted that the provision of Article 32z is directly transferred from the Article 7 DGA.

²⁴⁰ Ducuing and Papageorgiou (n 59).

²⁴¹ Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (OJ L 333/1, 27/12/2022).

²⁴² Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257/73 2882014).

Directive.²⁴³ The stated objectives are to reduce duplication, lower administrative burdens, and improve coordination among competent authorities, while explicitly leaving substantive reporting obligations unchanged. However, the operational design of the single-entry point raises a fundamental and unresolved problem under EU data protection law: the lack of a clear delineation of controller and processor roles²⁴⁴ in relation to the personal data processed within the reporting infrastructure itself.

The problem arises because the single-entry point is not merely a neutral transmission channel. It is a centrally developed, operated, and secured digital system, managed by ENISA, that receives, stores, and enables retrieval and supplementation of incident reports.²⁴⁵ These reports may contain personal data, particularly where they serve GDPR breach notification purposes or where cybersecurity incidents affect identifiable individuals. Yet Article 23a of the NIS 2 Directive provides only partial guidance on data governance. While it states that ENISA generally does not have access to the content of notifications unless an underlying legal act provides otherwise,²⁴⁶ it does not specify how this technical limitation translates into data protection roles under the GDPR. In particular, it does not clarify whether ENISA acts as a processor, or a joint controller.

This ambiguity is problematic because in the GDPR role allocation is functional, and not formal. Even if ENISA does not access the content of reports in the ordinary sense, it determines the means of processing by designing, operating, and securing the system, setting technical specifications, and enabling interoperability and authority-to-authority data flows. These activities go beyond mechanical transmission. At the same time, the competent authorities receiving the reports, data protection authorities, cybersecurity authorities, financial supervisors, or process the same data for different statutory purposes. The single-entry point thus creates a multi-actor, multi-purpose processing environment without explicitly mapping who controls which aspects of the processing and under what legal basis.

The absence of clear role allocation creates several risks. First, it undermines accountability. If personal data is over-collected, retained too long, or accessed by an authority beyond its mandate, it is unclear which actor bears responsibility under the GDPR. Second, it causes a risk to the exercise of data subject rights, as individuals affected by incidents may find it difficult to identify which authority is responsible for responding to access requests, complaints, or challenges relating to the processing of their personal data within the reporting system.

The role of ENISA is particularly sensitive. Article 23a(4) of the NIS 2 Directive limits ENISA's access to report content, reflecting a policy choice to avoid turning the Agency into a substantive incident intelligence. However, restricting access does not, by itself, resolve the question of controllership. ENISA designs the single-entry point, defines its technical and organisational measures, and ensures interoperability with other reporting systems, including those under the Cyber Resilience Act. These functions strongly suggest that ENISA exercises

²⁴³ Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (Text with EEA relevance) (L 333/164, 27/12/2022).

²⁴⁴ European Data Protection Board (EDPB), 'Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR' (2021).

²⁴⁵ Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance) (L 333/80, 27/12/2022) art 23(a). *ibid*.

²⁴⁶ NIS 2 Directive art 23(a)(4).

control over the means of processing, even if it does not determine the purposes of each report. Without clarification, ENISA risks occupying an ambiguous position that does not fit neatly into the GDPR's controller–processor dichotomy.²⁴⁷

The competent authorities, for their part, act as controllers when they receive and process reports within their statutory mandates. However, the single-entry point facilitates authority-to-authority sharing of information, which further complicates role allocation. When personal data is shared onward between authorities via the system, it becomes unclear whether each authority acts as an independent controller, whether there is a form of joint controllership, or whether the original recipient remains responsible for subsequent dissemination. The law currently provides no explicit answer.

Recommendations

The solution to this problem lies not in revising the core architecture of the single-entry point, but in explicitly articulating a layered controller model. First, the law or implementing guidance or organisational and technical arrangements²⁴⁸ should clarify that ENISA acts as a processor which is responsible for security, availability, and integrity of the system,²⁴⁹ but not for determining the purposes of processing incident data. This would align ENISA's role with its mandate and with the explicit limitation on access to report content. Second, competent authorities should be explicitly recognised as independent controllers for the personal data they receive and process through the single-entry point, each within the scope of their legal mandate. Third, authority-to-authority sharing enabled by the system should be governed by clear rules specifying when such sharing constitutes a new processing operation and which authority assumes controller responsibility at each stage.

We conclude that while the single-entry point represents a procedural simplification with clear systemic benefits, its current legal design leaves a gap in the allocation of data protection responsibilities. Without clarifying the respective responsibilities of ENISA and the competent authorities in relation to personal data, it causes a risk to the right to personal data protection. A clear, layered controller framework should complement the single entry-point mechanism to respect to right to personal data protection.

4.7 Trade secrets

Many of the regulations and directives tackled by the Digital Omnibus Proposal have revealed and handled structural tensions between the protection of confidential business information and data access rights. A common thread runs through these instruments: while trade secrets must not fundamentally limit data access rights, protective measures exist to preserve legitimate confidential interests. The Digital Omnibus Proposal does not seek to recalibrate this balance in a fundamental way. Instead, it introduces a series of targeted and relatively modest regulatory adjustments that clarify and fine-tune the position of trade secrets within the evolving regulatory framework for data. This chapter will examine these adjustments (or the lack thereof) for the (original) Data Act and Data Governance Act.

²⁴⁷ See for the analysis the expanding concept of controller and the case-law analysis, Alan Dahi and Marcelo Corrales Compagnucci, 'Device Manufacturers as Controllers – Expanding the Concept of "Controllership" in the GDPR' (2022) 47 Computer Law & Security Review 105762 <<https://doi.org/10.1016/j.clsr.2022.105762>>.

²⁴⁸ The arrangements mentioned in Article 23(a)(3) of the NIS 2 Directive.

²⁴⁹ NIS 2 Directive art 23(a)(2).

4.7.1 Trade secrets in the Data Act

As a preliminary matter, it should be noted that while the trade secret specific changes remain limited, the Digital Omnibus Proposal shapes ‘data secret’ sharing (i.e. sharing data that qualifies as trade secret) not only by trade secret-specific provisions but also by broader adjustments to data sharing obligations. Notably, the narrower B2G data sharing scope (see the discussion in section 4.4) – now limited to ‘public emergencies’ rather than ‘exceptional needs’ (Art. 1(5-19) Omnibus) – correspondingly reduces the situations where data secrets must be shared with public authorities (Art. 19(3) DA).

Problem 1: The proposal suffers some restructuring flaws.

The amendment to Article 19(3) itself (Art. 11(b) Digital Omnibus Proposal) remains limited to a technical correction, updating the cross-reference from Article 15 DA to Article 15a DA following the renumbering. A comparable restructuring exercise appears to have occurred in Article 21(5). Yet, the restructuring seems to have lost the reference to technical protection measures in (d), which is likely the result from inadvertence rather than a deliberate policy choice.

Recommendation

We suggest to reintroduce the reference to technical protection measures in Article 21(5) (d).

Problem 2: The additional refusal ground for third country sharing deserves more justification.

Relevant for trade secrets specifically, IoT-data sharing with third countries receives particular attention. The European Commission expresses concern that the ‘integrity and confidentiality’ of trade secrets may be compromised when exposed to ‘jurisdictions with inadequate protections or difficulties in their actual enforcement’ (rec. 10 Digital Omnibus Proposal). The Proposal therefore introduces an additional refusal ground applicable when there exists ‘a high risk of unlawful acquisition, use or disclosure to entities subject to regimes with inadequate protection, non-equivalent or weaker legal frameworks than the applicable Union rules’ or where appropriate enforcement in practice lacks (Art. 1(3) and (4); rec. 11 Digital Omnibus Proposal).

The added value to the existing refusal ground in case of high likelihood of serious economic damage (Art. 4(8) and 5(11); rec. 31 DA), also referred to in the proposal (rec. 11 Digital Omnibus Proposal), is questionable. This current exception in the DA also entrusts the risk assessment to the data holder and would have covered the instances where the risk third country related. The original articles even specifically refer to the (lack of) enforcement of trade secrets protection in third countries as an element in demonstrating the likelihood of serious economic damage.

The need for adding an additional refusal ground is not clear. The explanation in the recitals and the relevant staff working document remains rather limited, referring to strengthening trade secret protection through the cultivation of trust in the data economy and the reinforcement of legal predictability.²⁵⁰ This would reduce (legal and compliance) costs.²⁵¹ The staff working document also refers to ‘minimizing confidentiality breaches and mitigating the risk of data exploitation by third country free riders or the largest global tech companies’. Why

²⁵⁰ Rec. 13 Omnibus, SWD(2025) 836 final, 20.

²⁵¹ SWD(2025) 836 final, 20-21.

the existing refusal ground does not suffice, is not clear, especially as clarification (and thus legal certainty) could also flow from future interpretational guidelines from the EDIB, which would have been a more normal course of business in creating legal certainty for a legislative instrument as recent as the DA.

A possible, further explanation could be found in highlighting the (cyber)security goals that can be reached via these refusals. This would be in line with the original DA, as cybersecurity was already mentioned in the original recital 31 in this context (*'A possible negative impact on cybersecurity can be taken into account in that context.'*). It would also fit the EU's economic security policy in which 'preventing access to sensitive information and data that could undermine the EU's economic security' is considered a high-risk area worthy of a concentration of efforts.²⁵² Moreover, this policy mentions pursuing these objectives first by clarifying and improving existing tools.²⁵³ However, preparatory works do not explicitly connect this amendment to these goals.

Recommendation

We recommend the European Commission to define the relationship of the additional refusal ground with the existing refusal ground. This will enhance the predictability of both the original and additional refusal grounds for data holders and data users. We further suggest to explicitly anchor the additional refusal ground in the objectives of (cyber)security and the EU's economic security, and clearly articulate this rationale in the recitals or accompanying guidance (if this was indeed the intention). Framing it clearly as a security-driven instrument would strengthen its normative added value and would enhance policy transparency and accountability.

Problem 3: The proposal does not tackle the excessive blocking power of data holders under the IoT data sharing regime.

Under the IoT data sharing regime, data holders self-identify their trade secrets and the necessary measures to preserve the confidentiality of the trade secrets. This incentivises data holders to overclaim trade secret protection, so they can refuse, withhold or suspend data sharing.²⁵⁴ The Digital Omnibus Proposal recognises this concern in recital 14. However, it only mentions the (existing) 'safeguards against misuse of the refusal mechanism should remain in place, including the data holder's obligation to demonstrate in a duly substantiated manner that disclosure poses a high risk and to notify competent authorities'. No additional safeguards are installed. The recital explicitly states the decision and its demonstration should remain confidential, reinforcing trade secret protection and possibly locking out external legal advisors to assist users and/or third parties, who often find themselves already in a weaker bargaining position.

Recommendation

We urge the European to install additional safeguards against misuse of the refusal grounds and to reduce the ambiguity of the refusal grounds by interpretational guidelines and by

²⁵² Joint Communication to the European Parliament and the Council, Strengthening EU economic security, 10, <https://circabc.europa.eu/ui/group/7fc51410-46a1-4871-8979-20cce8df0896/library/777b1ecb-e7ce-4774-a92c-53f81e64ce76/details?open=true>.

²⁵³ Joint Communication to the European Parliament and the Council, Strengthening EU economic security, 14, <https://circabc.europa.eu/ui/group/7fc51410-46a1-4871-8979-20cce8df0896/library/777b1ecb-e7ce-4774-a92c-53f81e64ce76/details?open=true>.

²⁵⁴ SWD, 22; De Noyette, Margoni, Stähler, IIC 2025, (984) 990; Mylly, IIC 2024, (368) 384.

transparency of decisions by courts and/or intermediaries on this topic.²⁵⁵ Furthermore, we suggest that the European Commission clarifies that the confidentiality of the decision of the data holder and the substantiating demonstration do not impede external legal counsel.

4.7.2 Trade secrets in the Data Governance Act

The same preliminary comment made for the Data Act goes for the Data Governance Act. The incorporation of the DGA in the DA and the amendments coming with it, do not – for data secret sharing specifically – lead to significant changes. This does not mean that this aspect is not impacted indirectly by the overall changes, such as the lightening of the obligations of data intermediation service providers and data altruism organizations (*see section 4.3*).

Problem 1: The EDIB's role in developing guidelines (for trade secret protection) has lost its visibility.

Under the original wording of Article 30(d) DGA, the EDIB was entrusted with an express and substantive mandate 'to advise and assist the Commission with regard to developing consistent guidelines on how to best protect, in the context of this Regulation, commercially sensitive non-personal data, in particular trade secrets [...] from unlawful access'. This task was normatively significant: it singled out trade secret protection as a distinct regulatory concern within the governance of data re-use under the DGA. Article 30(e) and (h) also provided similar mandates for guidelines on cybersecurity and data spaces. Following the amendment, these explicit references have disappeared. The proposed Article 42 Data Act reframes the EDIB's role in more procedural and institutional terms. The earlier task is not entirely eliminated, but it is no longer autonomous or self-standing. Any attention to the protection of trade secrets (or cybersecurity/data spaces) must now be subsumed under the general task of supporting consistent application of the regulation, specifically in the context of consistent/good practice of and cooperation between competent authorities and Member States.

While distilling the enumeration of tasks can indeed serve the general objective of the Digital Omnibus Proposal to simplify the application of the Digital Acquis, the amendment as is, does not remain without meaning. The amendment marks a move from a substantive policy-guiding mandate towards a coordination- and enforcement-oriented role, with the consequence that these topics are treated as a horizontal enforcement concerns, rather than as topics warranting dedicated guidance at EDIB level. This could hinder the development of targeted, forward-looking interpretative guidance on trade secret and other concerns, precisely in areas where legal uncertainty and cross-border risks are most acute. By relegating these issues to the level of horizontal enforcement practice, the amendment risks diluting their normative visibility and reducing the EDIB's capacity to proactively shape a coherent Union-wide approach. In particular, it may weaken the EDIB's role as a forum for anticipating systemic risks linked to data re-use and international data sharing, and instead confine its contribution to ex post coordination, thereby limiting its added value in ensuring consistent, trust-enhancing safeguards under the data governance framework.

Recommendation

We propose that the proposed Article 42 DA explicitly confirms that the EDIB will assist the European Commission in the development of guidelines and standards.²⁵⁶ This will make sure

²⁵⁵ Ibid.

²⁵⁶ As also recommended in the Joint Declaration of the EDPB and the EDPS (page 46, nr. 170).

the EDIB can still play a sufficiently broad, anticipative role. We further suggest to reduce the now explicit, dispersed mandates for several topics to one general mandate for any topic concerning the (new version of the) Data Act,²⁵⁷ and to exemplify this general mandate with topics in areas where legal certainty is a specific concern, e.g. trade secret protection. This supports the goal of simplification, while maintaining visibility for these topics.

Problem 2: The proposal does not tackle the variety of confidentiality terms used in the DGA.

For the DGA, more than for the (original) Data Act, one of the biggest problems related to trade secrecy is the definitional conundrum. The use of the words 'related to trade secrets' is deliberate, as (a lot of) different confidentiality terms are used throughout the text.²⁵⁸ Examples are

- commercially confidential data,²⁵⁹
- commercially confidential information,²⁶⁰
- commercially sensitive data,²⁶¹
- competitively sensitive information,²⁶²
- protected data of non-personal nature,²⁶³
- protected know-how.²⁶⁴

Moreover, because of a lack of definitions for these different concepts, it is not clear how they relate to one another, although the legislature does indicate that each of these concepts encompasses the notion of a 'trade secret'. While this leaves an enormous room for improvement on the provisions related to trade secrets and would fit perfectly with the simplification goal of Omnibus, the regulation has not tackled this.

Recommendation

We urge the European Commission to limit the number of different confidentiality terms, and to limit their use to the instances where it is necessary to derogate from the concept of trade secrecy. Additionally, we suggest that all these concepts are sufficiently defined and clearly delineated from the other concepts, with a substantiation why a specific concept is used in a specific context.

²⁵⁷ This general mandate was also recommended in the Joint Declaration of the EDPB and the EDPS (page 47, nr. 171).

²⁵⁸ As presented by Lisa Van Dongen, in partnership with Kristina Irion, at the 19th Annual Conference of the European Policy for Intellectual Property Association: Intellectual Property and the Future of the Data Economy, Pisa, 2024, "EU Digital Regulation and Trade Secrets: Different Terms, Different Concepts?".

²⁵⁹ Rec. 6, 7, 9, 10, 42 DGA; Art. 5(8), 5(10) en 6(5)(c) DGA.

²⁶⁰ Rec. 15 DGA; Art. 3(1)(a), 5(3) en 7(4)(c) DGA.

²⁶¹ Rec. 19, 22, 23, 24 DGA; Art. 12(I) en 30(d) DGA.

²⁶² Rec. 37, 60 DGA.

²⁶³ Rec. 20 DGA; Art. 5(9) DGA.

²⁶⁴ Rec. 10 DGA; Art. 5(8) en 6(5)(c) DGA.

References

- Allen C, 'Verification (1:1) and Identification (1:N) Explanatory Graphics' (*Biometrics Institute*, 16 February 2024) <<https://www.biometricsinstitute.org/verification-11-and-identification-1n-explanatory-graphics/>> accessed 6 March 2026
- Article 29 Data Protection Working Party, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679' (2018) 17/EN WP251rev.01
- , 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679' (2018) 17/EN WP251rev.01
- Article 29 Working Party, 'Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is "Likely to Result in a High Risk" for the Purposes of Regulation 2016/679' (2017) wp248rev.01 <<https://ec.europa.eu/newsroom/article29/items/611236>> accessed 5 March 2026
- , 'Guidelines on Transparency under Regulation 2016/679' (2017) WP260 rev.01 <https://www.edpb.europa.eu/our-work-tools/our-documents/article-29-working-party-guidelines-transparency-under-regulation_en> accessed 5 March 2026
- Ausloos J, Mahieu R and Veale M, 'Getting Data Subject Rights Right: A Submission to the European Data Protection Board from International Data Rights Academics, to Inform Regulatory Guidance' (2019) 10 *Journal of Intellectual Property, Information Technology and E-Commerce Law (JIPITEC)* 283 <<https://doi.org/https://nbn-resolving.de/urn:nbn:de:0009-29-50315>>
- Baloup J and others, 'White Paper on the Data Governance Act' (2021)
- Bar-Siman-Tov I, 'An Introduction to the Comparative and Multidisciplinary Study of Omnibus Legislation' *Comparative Multidisciplinary Perspectives on Omnibus Legislation* (2021)
- Benifei B and Tudorache D, 'Report on the Proposal for a Regulation of the European Parliament and of the Council on Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts' (European Parliament, Committee on the Internal Market and Consumer Protection, Committee on Civil Liberties, Justice and Home Affairs 2023) P9_A(2023)0188_EN <[https://www.europarl.europa.eu/RegData/seance_pleniere/textes_deposes/rapports/2023/0188/P9_A\(2023\)0188_EN.pdf](https://www.europarl.europa.eu/RegData/seance_pleniere/textes_deposes/rapports/2023/0188/P9_A(2023)0188_EN.pdf)> accessed 6 March 2026
- Biagini G, 'Towards an AI-Literate Future: A Systematic Literature Review Exploring Education, Ethics, and Applications' (2025) 35 *International Journal of Artificial Intelligence in Education* 2616 <<https://doi.org/10.1007/s40593-025-00466-w>>
- Bieker F and Nolan K, 'European AI FOMO' [2026] *Verfassungsblog* <<https://doi.org/10.59704/8ea454b6677b517f>> accessed 5 March 2026
- Bitzenhofer F, 'Better Regulation Guidelines | Interoperable Europe Portal' (28 July 2024) <<https://interoperable-europe.ec.europa.eu/collection/assessments/document/better-regulation-guidelines>> accessed 5 March 2026
- 'Bonn Declaration on Freedom of Scientific Research' <https://www.bmftr.bund.de/SharedDocs/Downloads/EN/b/bonn_declaration_en.pdf?__blob=publicationFile&v=5> accessed 6 March 2026

Capgemini and others, 'Study Supporting the Evaluation of the Free Flow of Non-Personal Data Regulation, Open Data Directive and Data Governance Act' (European Commission 2025) <<https://data.europa.eu/doi/10.2759/8620781>> accessed 5 March 2026

Clifford D and Ausloos J, 'Data Protection and the Role of Fairness'

Council of Europe, 'Explanatory Report to the Protocol Amending the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data' (2018) Council of Europe Treaty Series-No. 223

Council of the European Union, 'Presidency Compromise Text on Omnibus VII – Digital (GDPR/P2B)' (2026) 6406/26 <https://www.euractiv.com/content/uploads/sites/2/2026/02/EURACTIV_OMNIBUS-1.pdf> accessed 6 March 2026

Craig P, 'Legal Certainty and Legitimate Expectations' in Paul Craig (ed), *EU Administrative Law* (Oxford University Press 2018) <<https://doi.org/10.1093/oso/9780198831655.003.0020>> accessed 5 March 2026

Dahi A and Corrales Compagnucci M, 'Device Manufacturers as Controllers – Expanding the Concept of “Controllership” in the GDPR' (2022) 47 Computer Law & Security Review 105762 <<https://doi.org/10.1016/j.clsr.2022.105762>>

De Hert P and Hajduk P, 'EU Cross-Regime Enforcement, Redundancy and Interdependence: Addressing Overlap of Enforcement Structures in the Digital Sphere After Meta.' (2024) 2024 Technology and Regulation 291 <<https://doi.org/10.71265/fydwsg59>>

Demetzou K, 'GDPR and the Concept of Risk: The Role of Risk, the Scope of Risk and the Technology Involved' in Eleni Kosta and others (eds), *Privacy and Identity Management. Fairness, Accountability, and Transparency in the Age of Big Data*, vol 547 (Springer International Publishing 2019) <https://doi.org/10.1007/978-3-030-16744-8_10> accessed 2 March 2026

Draghi M, 'The Future of European Competitiveness' (2024)

Drexel J and others, 'Position Statement of the Max Planck Institute for Innovation and Competition of 25 May 2022 on the Commission's Proposal of 23 February 2022 for a Regulation on Harmonised Rules on Fair Access to and Use of Data (Data Act)' (Max Planck Institute for Innovation and Competition 2022) <https://www.ip.mpg.de/fileadmin/ipmpg/content/stellungnahmen/Position_Statement_MPI_Data_Act_Formal__13.06.2022.pdf> accessed 5 March 2026

Ducuing C, 'A Legal Principle of Innovation? Need for an Assessment Against the Principle of Democracy' (2022) 14 Law, Innovation and Technology 237 <<https://doi.org/10.1080/17579961.2022.2113667>>

—, 'Data as a Contested Commodity' (2024) 24 Global Jurist 277 <<https://doi.org/10.1515/gj-2024-0065>>

—, *Data Commodification and the Law: Navigating Data Markets and Data Protection* (Intersentia 2025)

Ducuing C, Margoni T and Schirru L (eds), 'White Paper on the Data Act Proposal' (2022) <<https://www.law.kuleuven.be/citip/en/Publications/citip-whitepaperdataact.pdf>> accessed 5 March 2026

Ducuing C and Papageorgiou A, 'Commentary of Article 37 Data Act' *EU Data Law: A Commentary on the DGA and the DA* (Elgar 2026)

EDPB, 'Guidelines 01/2022 on Data Subject Rights - Right of Access'

<[https://www.edpb.europa.eu/system/files/2023-](https://www.edpb.europa.eu/system/files/2023-04/edpb_guidelines_202201_data_subject_rights_access_v2_en.pdf)

04/edpb_guidelines_202201_data_subject_rights_access_v2_en.pdf> accessed 2 March 2026

'EDPD-EDPS Joint Opinion 2/2026 On the Proposal for a Regulation as Regards the Simplification of the Digital Legislative Framework (Digital Omnibus)'

<[https://www.edpb.europa.eu/system/files/2026-](https://www.edpb.europa.eu/system/files/2026-02/edpb_edps_jointopinion_202602_digitalomnibus_en.pdf)

02/edpb_edps_jointopinion_202602_digitalomnibus_en.pdf> accessed 2 March 2026

European Commission, 'Better Regulation Guidelines' (European Commission 2021) SWD(2021) 305 final

—, 'Better Regulation Toolbox' (2023)

—, 'Communication from the Commission to the European Parliament and the Council Data Union Strategy Unlocking Data for AI' (2025) COM(2025) 835 final, 19/11/2025

— (ed), 'The Future of European Competitiveness: Part A: A Competitiveness Strategy for Europe' (Publications Office 2025) <<https://doi.org/10.2872/9356120>>

—, 'Proposal for a Directive of the European Parliament and of the Council Amending Directives 2006/43/EC, 2013/34/EU, (EU) 2022/2464 and (EU) 2024/1760 as Regards Certain Corporate Sustainability Reporting and Due Diligence Requirements' (2025) COM(2025) 81 final-2025/0045 (COD)

—, 'Annexes to the Proposal for a Regulation Amending Regulations (EU) 2016/1679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854, (EU) 2024/1689 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as Regards the Simplification of the Digital Legislative Framework, and Repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus) (1/2)' (2025) COM(2025) 837 final

—, 'Commission Staff Working Document Accompanying the Documents - Proposal for a Regulation Amending Regulations (EU) 2016/1679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854, (EU) 2024/1689 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as Regards the Simplification of the Digital Legislative Framework, and Repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus) - Amending Regulations (EU) 2024/1689 and (EU) 2018/1139 as Regards the Simplification of the Implementation of Harmonised Rules on Artificial Intelligence (Digital Omnibus on AI)' (2025) SWD(2025) 836 final

—, 'Proposal for a Regulation Amending Regulations (EU) 2016/1679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854, (EU) 2024/1689 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as Regards the Simplification of the Digital Legislative Framework, and Repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus)' (2025) COM(2025) 837 final 2025/0360 (COD) <<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52025PC0837>>

—, 'Proposal for a Regulation Amending Regulations (EU) 2016/1679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854, (EU) 2024/1689 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as Regards the Simplification of the Digital Legislative Framework, and Repealing

Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus)' (2025) COM(2025) 837 final 2025/0360 (COD)

—, 'Proposal for a Regulation of the European Parliament and of the Council Amending Regulations (EU) 2024/1689 and (EU) 2018/1139 as Regards the Simplification of the Implementation of Harmonised Rules on Artificial Intelligence (Digital Omnibus on AI)' (2025) COM(2025) 836 final-2025/0359 (COD) <<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52025PC0836>> accessed 26 January 2026

—, 'FAQs - Data Act' (2026)

<file:///C:/Users/u0170521/Downloads/FAQs_Data_Act_y6CNIhysdFESA1wcWyAFSnkao_108144.pdf>

—, '2025 - Commission Proposals (Omnibus Packages)'

<https://commission.europa.eu/document/download/9e358345-31e8-4cdd-8816-a30138ed07fe_en?filename=2025_%20Omnibus%20packages_List_for_Europa.pdf%3E>

—, 'Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions A Comprehensive Approach on Personal Data Protection in the European Union' COM(2010) 609 final, 4/11/2020 <<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52010DC0609>> accessed 5 March 2026

—, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions - Commission Work Programme 2026 - Europe's Independence Moment' COM(2025) 870 final, 21/10/2025

—, 'Ensuring EU Legislation Supports Innovation: The Innovation Principle as a Research and Innovation Tool for Innovation Friendly Regulation' <https://research-and-innovation.ec.europa.eu/law-and-regulations/ensuring-eu-legislation-supports-innovation_en> accessed 5 March 2026

European Data Protection Board, 'Study on the Secondary Use of Personal Data in the Context of Scientific Research' (2020) EDPS/2019/02-04 <https://www.edpb.europa.eu/system/files/2025-04/20250401_study_on_the_secondary_use_of_personal_data_in_the_context_of_scientific_research_23102020_en.pdf> accessed 6 March 2026

—, 'Lithuanian DPA: Fine Imposed on a Sports Club for Infringements of the GDPR in Processing of Fingerprints of the Customers and Employees |' (8 July 2021)

<https://www.edpb.europa.eu/news/national-news/2021/lithuanian-dpa-fine-imposed-sports-club-infringements-gdpr-processing_en> accessed 5 March 2026

European Data Protection Board (EDPB), 'Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR' (2021)

—, 'Guidelines 05/2022 on the Use of Facial Recognition Technology in the Area of Law Enforcement (Version 2.0)' (2023)

European Data Protection Board (EDPB) and European Data Protection Supervisor (EDPS), 'Joint Opinion 1/2026 on the Proposal for a Regulation as Regards the Simplification of the Implementation of Harmonised Rules on Artificial Intelligence (Digital Omnibus on AI)' (2026)

<https://www.edpb.europa.eu/system/files/2026-01/edpb_edps_jointopinion_202601_proposal_ai-omnibus_en.pdf> accessed 6 March 2026

—, ‘Joint Opinion 2/2026 on the Proposal for a Regulation as Regards the Simplification of the Digital Legislative Framework (Digital Omnibus)’ (2026)

—, ‘Opinion 2/2026 on the Proposal for a Regulation as Regards the Simplification of the Digital Legislative Framework (Digital Omnibus)’ (2026)

European Data Protection Supervisor (EDPS), ‘Towards A Digital Clearinghouse 2.0’ (2025) <https://www.edps.europa.eu/system/files/2025-01/towards_a_digital_clearinghouse_2_0_january_2025_en_0.pdf> accessed 21 February 2025

European Ombudsman, ‘Recommendation on the European Commission’s Compliance with “Better Regulation” Rules and Other Procedural Requirements in Preparing Legislative Proposals That It Considered to Be Urgent (983/2025/MAS - the “Omnibus” Case, 2031/2024/VB - the “Migration” Case, and 1379/2024/MIK - the “CAP” Case)’

Eustache L, Brousseau E and Toledano J, ‘The Economics of Data-Sharing: An Empirical Investigation of Data Sharing Ecosystems’ [2025] ICIS 2025 Proceedings <https://aisel.aisnet.org/icis2025/sharing_econ/sharing_econ/6>

Fernandes E, Holmes W and Zhgenti S, ‘Article 4 AI Literacy’ in Ceyhun Necati Pehlivan, Nikolaus Forgó and Peggy Valcke (eds), *The EU Artificial Intelligence (AI) Act - A Commentary* (Wolters Kluwer 2024)

Fia T and Maanen G van, ‘Through Thick and Thin: Data Commons, Community and the Struggle for Collective Data Governance’ (2025) 2025 Technology and Regulation 114 <<https://doi.org/10.71265/tk2x3d39>>

Figueiredo T, ‘AI Literacy Programs in Europe – Supporting Article 4 of the EU AI Act | EU Artificial Intelligence Act’ (23 May 2025) <<https://artificialintelligenceact.eu/ai-literacy-programs/>> accessed 6 March 2026

Graef I and Van Der Sloot B (eds), *The Legal Consistency of Technology Regulation in Europe* (1st edn, Hart Publishing 2024) <<https://doi.org/10.5040/9781509968053>>

Gutwirth S and Hert PD, ‘Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power’ (2021) 18 *Direito Público* <<https://doi.org/10.11117/rdp.v18i100.6200>> accessed 13 March 2026

‘ISO/IEC 2382-37:2022’ (ISO) <<https://www.iso.org/standard/73514.html>> accessed 6 March 2026

Jasserand C, ‘Legal Nature of Biometric Data: From “Generic” Personal Data to Sensitive Data’ (2016) 2 *European Data Protection Law review* <<https://doi.org/10.21552/EDPL/2016/3/6>>

Kindt EJ, ‘Having Yes, Using No? About the New Legal Regime for Biometric Data’ (2018) 34 *Computer Law & Security Review* 523 <<https://doi.org/10.1016/j.clsr.2017.11.004>>

Kun E, ‘Searching for the Appropriate Legal Basis for Personal Data Processing for Cybersecurity Purposes Under the NIS 2 Directive: Legal Obligation and/or Legitimate Interest?’ (2025) 56 *Computer Law & Security Review* 106098 <<https://doi.org/10.1016/j.clsr.2024.106098>>

Kuner C and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020) <<https://doi.org/10.1093/oso/9780198826491.001.0001>> accessed 5 March 2026

Lazarotto B, 'The Data Omnibus: The Good, the Bad, and The Ugly Behind the DGA and Data Act Rewrite' (*MediaLaws*, 19 December 2025) <<https://www.medialaws.eu/the-data-omnibus-the-good-the-bad-and-the-ugly-behind-the-dga-and-data-act-rewrite/>> accessed 6 March 2026

'Lithuania: VDAI Fines Praktiškas €6,000 for Unlawful Processing of Personal Data | News' (*DataGuidance*, 13 January 2023) <<https://www.dataguidance.com/news/lithuania-vdai-fines-praktiskas-eu6000-unlawful>> accessed 5 March 2026

Lopez CAF, 'Against Biometric Identifiability: Part I: The Law of What Is Reasonably Likely' (2026) 11 *European Data Protection Law Review* 465 <<https://doi.org/10.21552/edpl/2025/4/10>>

Martin AK and Whitley EA, 'Fixing Identity? Biometrics and the Tensions of Material Practices' (2013) 35 *Media, Culture & Society* 52 <<https://doi.org/10.1177/0163443712464558>>

Naudts L, Dewitte P and Ausloos J, 'Meaningful Transparency Through Data Rights: A Multidimensional Analysis' *Research Handbook on EU Data Protection Law* (Edward Elgar Publishing 2022)

NOYB, 'Digital Omnibus: First Analysis of Select GDPR and ePrivacy Proposals by the European Commission (Version 3.0)' (2026) <<https://noyb.eu/sites/default/files/2025-12/noyb%20Digital%20Omnibus%20Report%20V1.pdf>> accessed 5 March 2026

Nusselder S, 'Scrutinising the Interplay between Data Protection and Cybersecurity: A Paradox Shrouded Behind the "State-of-the-Art"' (2025) 2 *European Data Protection Law Review*

Purtova N and van Maanen G, 'Data as an Economic Good, Data as a Commons, and Data Governance' (2023) 16 *Law, Innovation and Technology* 1 <<https://doi.org/10.1080/17579961.2023.2265270>>

Purtova NP, 'Why Simply Redefining Personal Data Narrowly Does Not Solve the Problem of the "Law of Everything"' (*Brussels Privacy Hub*, 15 December 2025) <<https://brusselsprivacyhub.com/why-simply-redefining-personal-data-narrowly-does-not-solve-the-problem-of-the-law-of-everything/>> accessed 2 March 2026

Rakibul Hasan Chowdhury and others, 'The Role of Predictive Analytics in Cybersecurity: Detecting and Preventing Threats' (2024) 23 *World Journal of Advanced Research and Reviews* 1615 <<https://doi.org/10.30574/wjarr.2024.23.2.2494>>

Skioitytė G and Sadauskaitė A, 'A Digital Omnibus: Identifying Interlinks and Possible Overlaps Between Different Legal Acts in the Field of Digital Legislation to Streamline Tech Rules' (European Parliament 2026) Study requested by the IMCO committee PE 772.641 <[https://www.europarl.europa.eu/RegData/etudes/STUD/2026/772641/ECTI_STU\(2026\)772641_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2026/772641/ECTI_STU(2026)772641_EN.pdf)> accessed 6 March 2026

Sumer B, 'When Do the Images of Biometric Characteristics Qualify as Special Categories of Data Under the GDPR? A Systemic Approach to Biometric Data Processing' *2022 International Conference of the Biometrics Special Interest Group (BIOSIG)* (2022) <<https://doi.org/10.1109/BIOSIG55365.2022.9897034>> accessed 6 March 2026

Sumer B, 'The AI Act's Exclusion of Biometric Verification: Minimal Risk by Design and Default?' (2024) 10 *European Data Protection Law Review* 150 <<https://doi.org/10.21552/edpl/2024/2/6>>

Sumer B and others, 'AI Acts' Ripple Effect on Biometric Data: Harmonising or Fragmenting the Regulation of Biometric Data' in Kostina Prifti and others (eds), *Digital Governance: Confronting the*

Challenges Posed by Artificial Intelligence (TMC Asser Press 2024) <https://doi.org/10.1007/978-94-6265-639-0_8>

UNESCO, 'Recommendation on Science and Scientific Researchers (13 November 2017) SHS/BIO/PI/2017/3 Rev'

—, 'Recommendation on the Ethics of Artificial Intelligence (23 November 2021) SHS/BIO/PI/2021/1' <<https://unesdoc.unesco.org/ark:/48223/pf0000381137>> accessed 6 March 2026

Wolff HA, Brink S and Ungern-Sternberg A von (eds), 'Artikel 15 Außergewöhnliche Notwendigkeit Der Datennutzung' *BeckOK Datenschutzrecht: DS-GVO, BDSG, Grundlagen, Bereichsspezifischer Datenschutz - Kommentar* (51st edn, CH BECK 2025)

Meroni & Co, Industrie Metallurgiche, SpA v High Authority of the European Coal and Steel Community [1958] ECJ Case 9-56, ECLI:EU:C:1958:7

Charter of Fundamental Rights of the European Union 2000 (2000/C 364/01)

The Queen, on the application of Vodafone Ltd and Others v Secretary of State for Business, Enterprise and Regulatory Reform [2010] ECJ Case C-58/08

European Parliament v Council of the European Union [2012] ECJ Case C-355/10, ECLI:EU:C:2012:516

Consolidated version of the Treaty on the Functioning of the European Union 2012 (OJ C326/47)

Smaranda Bara and Others v Casa Națională de Asigurări de Sănătate and Others [2015] ECJ Case C-201/14

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA 2016 (OJ L)

Patrick Breyer v Bundesrepublik Deutschland [2016] ECJ Case C-582/14

Republic of Poland v European Parliament and Council of the European Union [2018] ECJ Case C-5/16

Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (recast) 2019 (OJ L 172/56, 20/6/2019)

[2020] AG Kerpen 106 C 96/20

[2021] Rb Amsterdam C/13/687315 / HA RK 20-207 ECLI:NL:RBAMS:2021:1020
ECLI:NL:RBAMS:2021:1020

[2021] Rb Amsterdam C/13/689705 / HA RK 20-258 ECLI:NL:RBAMS:2021:1019

[2021] Rb Rotterdam ROT 19/5030, ECLI:NL:RBROT:2021:2306

[2021] Rb Limburg ECLI:NL:RBLIM:2021:2946

[2022] Raad van State 202006960/1/A3 ECLI:NL:RVS:2022:2403

[2022] LG Gießen 2 O 186/22

[2022] Rechtbank Zeeland-West-Brabant AWB- 21_1058 ECLI:NL:RBZWB:2022:5975

[2023] Landesrechtsportal Brandenburg 11 U 332/22 ECLI:DE:OLGBB:2023:0929.11U332.22.00

FT (Copies du dossier médical) [2023] ECJ Case C-307/22 ECLI:EU:C:2023:811

Gesamtverband Autoteile-Handel eV v Scania CV AB [2023] ECJ Case C-319/22

OQ v Land Hessen (C-634/21) [2023] ECJ C-634/21, ECLI:EU:C:2023:957

VK and Others v BMW Bank GmbH and Others [2023] Court of Justice Joined Cases C-38/21, C-47/21, C-232/21, ECLI:EU:C:2023:1014

IAB Europe v Gegevensbeschermingsautoriteit [2024] ECJ Case C-604/22

OC v European Commission [2024] ECJ Case C-479/22 P ECLI:EU:C:2024:215

HP - Hrvatska pošta dd v Povjerenik za informiranje [2024] ECJ Case C-336/23

[2024] OLG Düsseldorf 6 U 114/23

Österreichische Datenschutzbehörde v F R [2025] ECJ Case C-416/23 ECLI:EU:C:2025:3

[2025] LAG München 2 SLa 70/25

European Data Protection Supervisor v Single Resolution Board [2025] ECJ Case C-413/23 P ECLI:EU:C:2025:645

Decision 41/2025 [2025] Greek Data Protection Authority 41/2025

[2025] BGH I ZR 115/25

Charter of Fundamental Rights of the European Union (OJ C 326/392, 26/10/2012)

Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules (OJ L 328/7, 18/12/2019)

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance) (L 333/80, 27/12/2022)

Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (Text with EEA relevance) (L 333/164, 27/12/2022)

Interinstitutional Agreement between the European Parliament, the Council of the European Union and the European Commission on Better Law-Making (OJ L 123/1, 12/5/2016)

International Covenant on Economic, Social and Cultural Rights (adopted 16 December 1966, entered into force 3 January 1976) 993 UNTS 3

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free

movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4/5/2016)

Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (Text with EEA relevance.) (OJ L 295/39, 23/10/2018)

Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011 (Text with EEA relevance) (OJ L 169/1, 20/6/2019)

Regulation (EU) 2019/1243 of the European Parliament and of the Council of 20 June 2019 adapting a number of legal acts providing for the use of the regulatory procedure with scrutiny to Articles 290 and 291 of the Treaty on the Functioning of the European Union (Text with EEA relevance) (OJ L 198/241, 20/6/2019)

Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance) (OJ L 277/1, 19/10/2022)

Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (OJ L 333/1, 27/12/2022)

Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act) (Text with EEA relevance) (OJ L 2023/2854, 13/12/2023)

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (OJ L, 12/7/2024)

Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257/73 28/8/2014)

Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (Text with EEA relevance) (OJ L 152/1, 30/5/2022)

Universal Declaration of Human Rights (adopted 10 December 1948) 217 A (III)

Convention for the Protection of Human Rights and Fundamental Freedoms 1950

European Convention on Human Rights 1950

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981 (European Treaty Series - No 108)

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981, ETS 108 1981

Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 223) 2018

Charter of Fundamental Rights of the European Union (OJ C 326/392, 26/10/2012)

Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257/73 28/8/2014)

Aan de Staatsecretaris van Economische Zaken - Digitale Economie en
Soevereiniteit

Directoraat-generaal
Economie en Digitalisering
Directie Digitale Economie

Auteur
[Redacted]

TER BESLISSING
Datum aangemaakt
2 april 2026

Kenmerk
DGED-DE / 105571684

nota
TER BESLISSING

Start consultaties concept uitvoeringswet AI-
verordening en verzenden Kamerbrief

Kopie aan
[Redacted]

Bijlage(n)
3

Parafenroute

[Redacted signature area]

Aanleiding

- De concept uitvoeringswet AI-verordening (UAIV) en bijbehorende memorie van toelichting (MvT) ter uitvoering van de AI-verordening zijn klaar voor openbare consultatie.
- Op 29 september 2025 is toegezegd dat de Tweede Kamer wordt geïnformeerd over de voorgenomen inrichting van het toezicht op de AI-verordening in Nederland.

Geadviseerd besluit

- Instemmen met de concept UAIV en MvT en deze in consultatie brengen.
- Instemmen met de Kamerbrief over het AI-toezichtstelsel en deze verzenden aan de Tweede Kamer.

Kernpunten

- De Europese AI-verordening is op 2 augustus 2024 in werking getreden.
- Lidstaten moeten onder andere één of meer markttoezichtautoriteiten aanwijzen voor het toezicht op naleving van de verordening. Het uitvoeringswetsvoorstel regelt welke autoriteiten hiervoor worden aangewezen (bijlage 1) en de gemaakte keuzes worden toegelicht in de Memorie van Toelichting (bijlage 2).
- De start van de consultatiefase over de concept UAIV en MvT is het sluitstuk van een uitgebreid afstemmingsproces met tien betrokken departementen, alle relevante toezichthouders en allerlei belanghebbenden.

- Voor wetgeving gelden verschillende toetsen. Een openbare internetconsultatie is voor EU-uitvoeringswetgeving niet vereist, maar wordt in dit geval wenselijk geacht vanwege de maatschappelijke aandacht voor het onderwerp AI. Het gaat verder om het vragen van de verplichte (uitvoerings)toetsen aan o.m. de beoogd markttoezichtautoriteiten ten aanzien van onder meer de uitvoerbaarheid, wetgevingskwaliteit en regeldruk.
- Na deze consultatieronde wordt het wetsvoorstel nog twee keer aan u voorgelegd, rond de zomer voor behandeling in de MR met het oog op advisering door de Raad van State (RvS) en na verwerking van het advies van de RvS voor aanbieding aan de Tweede Kamer.
- Een Kamerbrief over het AI-toezicht in Nederland is opgesteld om aan meerdere toezeggingen hierover te voldoen (bijlage 3). Deze brief wordt door u mede namens de staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties, de staatssecretaris van Justitie en Veiligheid, de minister van Financiën, de minister van Sociale Zaken en Werkgelegenheid, de minister van Volksgezondheid, Werkgelegenheid en Sport en de minister van Infrastructuur en Waterstaat aan de Kamer gestuurd.

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**
Directie Digitale Economie

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

Ons kenmerk
DGED-DE / 105571251

Bijlage(n)
2

Datum 20 april 2026
Betreft Inrichting toezicht op de naleving van de AI-verordening

Geachte Voorzitter,

Met deze brief informeer ik u, mede namens de staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties, de staatssecretaris van Justitie en Veiligheid, de minister van Financiën, de minister van Sociale Zaken en Werkgelegenheid, de minister van Volksgezondheid, Welzijn en Sport en de minister van Infrastructuur en Waterstaat, over de wijze waarop het kabinet voornemens is het toezicht op de naleving van de Europese AI-verordening vorm te geven. Hiermee geef ik invulling aan de toezegging van 29 september 2025 om u te informeren nadat het kabinet hierover een besluit heeft genomen. De internetconsultatie over de uitvoeringswet AI-verordening, waarin deze inrichting wordt voorgesteld, loopt gedurende 6 weken na de publicatiedatum op <https://www.internetconsultatie.nl/uaiv>.

Kunstmatige intelligentie, ofwel AI, is een systeemtechnologie en wordt steeds breder ingezet in vrijwel alle sectoren en domeinen. De technologie verandert de aard en vorm van ons werk, fabrieksprocessen worden op nieuwe manieren geautomatiseerd en voor een steeds groter aantal mensen maakt contact met AI een regulier onderdeel uit van hun dagelijks leven. De kansen en beloften van AI zijn groot, maar kunnen alleen benut worden als er vertrouwen bestaat vanuit burgers, bedrijven en de samenleving als geheel. De Europese AI-verordening moet ervoor zorgen dat men kan rekenen op de veiligheid en betrouwbaarheid van de AI-systemen waar een steeds groter deel van onze data en processen aan worden toevertrouwd.

De verordening is op 1 augustus 2024 in werking getreden. Het toezicht op de naleving van de AI-verordening moet grotendeels nationaal worden ingericht. Door de domein- en sectoroverstijgende aard van AI vergt het toezicht op de AI-verordening een samenspel van een groot aantal toezichthouders over de breedte van de samenleving. Het gaat om een belangrijke nieuwe wettelijke taak die nog niet is belegd, maar die gedeeltelijk aansluit bij een aantal bestaande toezichtstaken.

Het kabinet heeft ervoor gekozen om het toezicht zorgvuldig vorm te geven, met oog voor de gewenste toezichtspraktijk door de toezichthouders. Hierbij heeft het kabinet de consequentie geaccepteerd dat de Nederlandse uitvoeringswet naar verwachting later in werking treedt dan momenteel wordt voorgeschreven vanuit

de AI-verordening. Kanttekening hierbij is dat de data waarop een aantal bepalingen van toepassing wordt waarschijnlijk naar achteren zullen schuiven in de tijd als gevolg van de onderhandelingen over de AI-omnibus.¹ Later in deze brief wordt nader ingegaan op het tijdpad. Ook wordt beschreven hoe invulling zal worden gegeven aan de financieringsvraagstukken rondom dit toezicht.

Kern AI-verordening

Het doel van de AI-verordening is om de ontwikkeling en toepassing van veilige en betrouwbare AI-systemen te bevorderen, om de grondrechten van EU-burgers te beschermen en om innovatie te stimuleren. De verordening draagt bij aan het versterken van het vertrouwen in AI-systemen en positioneert de Europese Unie als een betekenisvolle speler op het gebied van betrouwbare en mensgerichte AI. Hiermee wordt een solide basis gelegd voor een digitale samenleving waarin technologische vooruitgang en publieke waarden hand in hand gaan. De AI-verordening doet dit door in de hele EU gelijke eisen te stellen aan ontwikkelaars en gebruiksverantwoordelijken van bepaalde AI-systemen, namelijk wanneer ontwikkeling en gebruik ervan tot hoge risico's zou kunnen leiden voor onze veiligheid, gezondheid of fundamentele rechten. De AI-verordening is risico-gebaseerd omdat de eisen zijn afgestemd op de mate van risico die de AI vormt voor veiligheid, gezondheid of fundamentele rechten: hoe hoger het risico, hoe strenger de eisen. Daarmee wordt geborgd dat er alleen regels zijn waar nodig, en dat de ruimte voor innovatie zo groot mogelijk blijft. De AI-verordening reguleert verschillende categorieën AI-systemen en het gebruik ervan:

- **Verboden AI-praktijken:** de verordening benoemt een aantal AI-praktijken die zulke ernstige negatieve gevolgen hebben, dat ze verboden zijn. Hieronder vallen bijvoorbeeld het verbod op manipulatieve AI en het ongericht scrapen van gezichtsafbeeldingen met behulp van AI (deze bepalingen zijn in februari 2025 van kracht geworden);
- **Hoog-risico AI-systemen** waarvoor eisen aan de ontwikkeling en het gebruik ervan worden gesteld, zoals databeheer en risicomanagement. Hieronder vallen:
 - AI-systemen als product of veiligheidscomponent van producten die reeds gereguleerd zijn in de EU en onder die regelgeving al keuring door een externe partij moeten ondergaan. Bijvoorbeeld bepaalde machines of medische hulpmiddelen;
 - AI-systemen als toepassing binnen één van de acht hoog-risico toepassingsgebieden van de AI-verordening. Bijvoorbeeld beoordelingen binnen het onderwijs of het verlenen van essentiële particuliere of publieke diensten. De toepassing van AI-systemen

¹ In november 2025 heeft de Europese Commissie een voorstel gepubliceerd met wijzigingen van onder andere de AI-verordening (de zgn. AI-omnibus) met als primaire doelstelling het vereenvoudigen van de nalevingslasten door het bedrijfsleven zonder de doelen van de wetgeving aan te tasten. Naar verwachting volgen na de onderhandelingen in 2026 enkele wijzigingen van de AI-verordening die de nalevingslast verminderen. Waar nodig en mogelijk, zullen deze wijzigingen meegenomen worden in het wetsvoorstel.

in deze gebieden kan waardevol zijn, maar ook tot reële risico's voor de gezondheid, veiligheid of fundamentele rechten zorgen.

- Transparantie-eisen: wanneer mensen direct in contact staan met AI-systemen (zoals chatbots en generatieve AI), moet duidelijk gemaakt worden dat degene die met AI praat, wordt blootgesteld aan emotieherkenning of biometrische categorisatie of dat content AI-gegenereerd is (zoals bij deepfakes);
- AI-modellen voor algemene doeleinden: dit zijn modellen die voor veel verschillende toepassingen gebruikt kunnen worden en geïntegreerd worden in AI-systemen.

Toezichtgebieden AI-verordening

- De Europese Commissie zal toezicht houden op AI-modellen voor algemene doeleinden, zoals de modellen achter bekende chatbots, waaronder ChatGPT en Gemini. Voor het toezicht op alle andere categorieën verplicht de AI-verordening lidstaten om zelf één of meer markttoezichtautoriteiten aan te wijzen.
- Voor het toezicht op bestaande productregulering en het toezicht op financiële instellingen wordt in de AI-verordening aangegeven welke toezichthouder op de naleving ervan toeziet. Daar kan onderbouwd van worden afgeweken, maar het kabinet ziet daar geen redenen voor.
- Voor toezichttaken op het gebied van rechtshandhaving, migratie-, asiel- en grenstoezichtbeheer, rechtsbedeling en democratische processen stelt de verordening specifieke eisen aan de markttoezichtautoriteit, met name aan de mate van onafhankelijkheid. Met al deze randvoorwaarden is rekening gehouden bij de voorgenomen inrichting van het toezicht.
- Verder moet in iedere lidstaat één van de markttoezichtautoriteiten als centraal contactpunt zijn aangewezen waar iedereen met vragen over toezicht op de AI-verordening terecht kan.
- Een deel van de hoog-risico AI-systemen moet verplicht door derde partijen (aangemelde instanties) gecertificeerd worden. De lidstaat moet aanmeldende autoriteiten aanwijzen die deze partijen kunnen beoordelen en erkennen. Deze aangemelde instanties beoordelen of AI-systemen voldoen aan de vereisten van de verordening. Als dat het geval is, certificeren ze die systemen.
- Tot slot moet elke lidstaat een lijst publiceren waarin staat welke autoriteiten op het grondgebied reeds opereren als grondrechtenautoriteiten. Dit heeft het kabinet in het najaar van 2024 gedaan. De grondrechtenautoriteiten en markttoezichthouders kunnen in specifieke gevallen informatie uitwisselen en samenwerken.

Advies van de toezichthouders

Omdat AI breed wordt ingezet, hebben veel toezichthouders al met AI te maken vanuit hun bestaande taken en bevoegdheden. Zo kan de Autoriteit Consument en Markt (ACM) al ingrijpen wanneer algoritmes worden gebruikt om consumenten te

misleiden en kan de Rijksinspectie Digitale Infrastructuur (RDI) al toezien op algoritmes die worden gebruikt voor de stabiliteit en veiligheid van telecomnetwerken. De Autoriteit Persoonsgegevens (AP) heeft al ruime handhavende bevoegdheden vanuit de Algemene verordening gegevensbescherming (AVG) om in te grijpen wanneer een (voorgenomen) verwerking van persoonsgegevens voor of door algoritmes niet rechtmatig, behoorlijk of transparant plaatsvindt. De AI-verordening is aanvullend op een bestaand veld van regelgeving en toezicht.

Om de AI-verordening zo goed mogelijk in het bestaande veld van toezicht in te bedden, heeft het kabinet de Directie Coördinatie Algoritmes (DCA) van de AP en de RDI gevraagd om in afstemming met alle betrokken toezichthouders een advies uit te brengen over hoe het toezicht op de naleving van de AI-verordening het beste kan worden vormgegeven. Aan de hand van het beleidskompas en met dit advies van de toezichthouders als uitgangspunt is het voorgenomen toezichtstelsel op de AI-verordening tot stand gekomen. Het advies van de toezichthouders is grotendeels overgenomen door het kabinet.

Samenvatting toezichtstelsel AI-verordening

In het ontwerp van het toezicht heeft het kabinet meerdere belangen verenigd. Allereerst wordt zo veel mogelijk herkenbaarheid voor organisaties die onder de regels vallen beoogd, door aan te sluiten bij toezichthouders die zij al kennen. Daarnaast wordt voor het toezicht op gebieden zonder bestaande, herkenbare toezichthouder gekozen om het toezicht centraal te beleggen bij één toezichthouder. Tevens is beoogd dat via sterke coördinatie en kennisopbouw uniforme naleving van de AI-verordening in Nederland en kennisdeling tussen sectorale toezichthouders tot stand komt.

Dit mondt uit in het kabinetsvoorstel om tien markttoezichtautoriteiten aan te wijzen voor het toezicht op de naleving van de AI-verordening. Iedere markttoezichtautoriteit houdt toezicht op de ontwikkeling, het op de markt brengen en het gebruik van die systemen binnen de gebieden waarvoor die markttoezichtautoriteit is aangewezen. De coördinatie en kennisdeling wordt verzorgd door de samenwerking tussen AP en RDI. Dit voorstel is gebaseerd op de volgende overwegingen:

- Waar mogelijk en gewenst wordt voorgesteld om aan te sluiten bij bestaande expertise en bevoegdheden van toezichthouders. Dit is het geval voor toezicht op AI in de kritieke infrastructuur (RDI en ILT), op AI voor financiële dienstverlening door financiële instellingen (AFM en DNB) en op AI in producten die onder bestaande productregelgeving vallen (NVWA, NLA, ILT, RDI en IGJ). Voor het toezicht op hoog-risico AI-systemen die worden ontwikkeld en gebruikt door de rechtbanken, de gerechtshoven, de Hoge Raad, de Centrale Raad van Beroep, het College van Beroep voor het bedrijfsleven en het parket bij de Hoge Raad in de rechtsbedeling wordt de procureur-generaal bij de Hoge Raad (PGHR) aangewezen, en voor het toezicht op die systemen die worden ontwikkeld en gebruikt door de Afdeling bestuursrechtspraak van de Raad van State (ABRVs) wordt de voorzitter van de ABRV's

aangewezen. Organisaties binnen die gebieden houden daarmee contact met de voor hen reeds bekende toezichthouders, ook als het over AI gaat.

- Voor de toezichtgebieden uit de AI-verordening die niet goed aansluiten op bestaande bevoegdheden van toezichthouders, wordt voorgesteld om de AP als markttoezichtautoriteit aan te wijzen. Dit gaat om een groot deel van de hoog-risico toepassingsgebieden, de transparantieplichtingen en de verboden AI-praktijken. Deze categorieën sluiten aan bij de bestaande expertise van de AP op het gebied van sector- en domeinoverstijgend toezicht en toezicht op de AVG. Daarnaast heeft het de voorkeur van het kabinet om deze gebieden bij één markttoezichtautoriteit te beleggen om verdere versnippering van het AI-verordening toezicht te voorkomen.

Aangezien het toezicht op de naleving van AI-verordening over verschillende sectoren en domeinen verdeeld is en aan meerdere bestaande taken en bevoegdheden raakt, zullen de aangewezen markttoezichtautoriteiten onderling en met andere relevante autoriteiten effectief en efficiënt moeten samenwerken. Om deze samenwerking te ondersteunen, gezamenlijk kennis op te bouwen en zo veel mogelijk uniform toezicht te waarborgen wordt voorgesteld om de RDI en de AP coördinerende taken te geven.

Een belangrijk deel van het AI-toezicht op de AI-verordening wordt bij de AP belegd. Hiervoor wordt de AP een markttoezichtautoriteit. Het kabinet kiest ervoor om het toezicht op de AI-verordening binnen de AP zelfstandig, onafhankelijk van en nevensgeschikt ten opzichte van het toezicht op de AVG te beleggen, met een aanspreekpunt voor toezicht op de AI-verordening in het bestuur en naar de buitenwereld. In de beoogde inrichting heeft deze bestuurder een instemmingsvereiste voor besluiten in het kader van het toezicht op de AI-verordening.

In bijlage 1 bij deze brief wordt per onderdeel van de AI-verordening nadere toelichting gegeven op de voorgenomen keuze voor de markttoezichtautoriteiten, aanmeldende autoriteiten en de reeds geïdentificeerde grondrechtenautoriteiten. Bijlage 2 betreft een visuele weergave van het voorgenomen toezichtstelsel.

Financiering van het toezicht

Het toezicht op de naleving van de AI-verordening betreft grotendeels nieuwe taken voor de beoogd markttoezichtautoriteiten. Het is van belang dat toezichthouders in staat worden gesteld deze nieuwe taken adequaat uit te voeren. Dit kan betekenen dat aanvullende financiële middelen nodig zijn of dat herprioritering binnen bestaande middelen wordt overwogen voor de uitvoering van deze taken.

Door de voorgenomen markttoezichtautoriteiten worden de financiële consequenties en de haalbaarheid en uitvoerbaarheid van deze nieuwe toezichtstaken in kaart gebracht.

Tijdpad

Een goede naleving van de AI-verordening vraagt om een samenspel tussen de Europese Commissie, het kabinet, de markttoezichtautoriteiten en de ondertoezichtgestelden. De inrichting van het toezicht op de AI-verordening betreft een nieuw stelsel in Nederland waarin veel bestaande autoriteiten met elkaar zullen moeten samenwerken. Zoals eerder aangegeven heeft het kabinet ervoor gekozen om het toezicht zorgvuldig vorm te geven en de consequentie geaccepteerd dat de uitvoeringswet mogelijk later gereed is dan op dit moment wordt voorgeschreven vanuit de AI-verordening.

Parallel aan de internetconsultatie worden alle verplichte toetsen uitgevoerd. Dat zijn in ieder geval de uitvoerings- en handhavingstoetsen van alle beoogde markttoezichtautoriteiten, de wetgevingstoets van JenV, het wetgevingsadvies van de AP, de toets door het Adviescollege Toetsing Regeldruk en de toets door de Raad voor de Rechtspraak.

Na ontvangst van alle reacties wordt een aangepaste versie van het wetsvoorstel en de bijhorende memorie van toelichting aan de Ministerraad voorgelegd met het oog op aanbieding daarvan aan de Raad van State voor advies.

Na verwerking van het advies van de Raad van State en wanneer het wetsvoorstel volledig van dekking is voorzien kan het bij uw Kamer worden ingediend.

Na behandeling en goedkeuring door Tweede en Eerste Kamer en publicatie en inwerkingtreding van de uitvoeringswet hebben de markttoezichtautoriteiten formeel de taak om toezicht te houden op de naleving van de AI-verordening en beschikken zij over de voorgeschreven bevoegdheden.

Het feit dat de uitvoeringswet waarschijnlijk niet tijdig in werking treedt, wil niet zeggen dat daardoor de verplichtingen uit de verordening nog niet gelden, want de verordening is rechtstreeks toepasselijk in alle lidstaten.

Het kabinet verwacht dat AI de komende jaren een steeds belangrijkere rol gaat spelen in de maatschappij. Om burgers en bedrijven ten volste van de kansen van AI te laten profiteren, moeten zij kunnen vertrouwen op de veiligheid van die AI-producten en -systemen.

W.J.M. Aerdt
Staatssecretaris van Economische Zaken en Klimaat

Bijlage 1 - Toelichting toezichtstelsel AI-verordening

Hieronder wordt per onderdeel van de AI-verordening nadere toelichting gegeven op de voorgenen keuze voor de (markt)toezichthouder(s).

Centraal contactpunt en coördinatie van AI-toezicht

De verordening schrijft in artikel 70 voor dat er één markttoezichtautoriteit wordt aangewezen als centraal contactpunt (single point of contact) voor zowel de Commissie als binnen de lidstaat. Deze taak wordt bij de RDI belegd. De RDI en de AP borgen samen de coördinatie tussen en samenwerking met alle betrokken toezichthouders. Dit moet een eenduidige uitleg en toepassing van de verordening bevorderen, het delen van goede praktijken vergemakkelijken en het gezamenlijk optrekken bij onderzoeken mogelijk maken.

Toezicht op verboden AI-praktijken

Een aantal verboden AI-praktijken, zoals manipulatie of gebruik maken van kwetsbaarheden, kan binnen elk domein plaatsvinden. Het kan ook plaatsvinden in domeinen waarvoor nu geen sectorale toezichthouder is aangewezen. Manipulatie of gebruik van kwetsbaarheden vindt vaak, maar niet altijd, plaats door het gebruik van persoonsgegevens. Dat maakt dat er ook een relatie kan zijn met toezicht op de AVG.

Om versnippering van het toezicht te voorkomen en zo goed als mogelijk aan te sluiten bij bestaande expertise en bevoegdheden, is het kabinet voornemens om de AP aan te wijzen als markttoezichtautoriteit voor alle verboden AI-praktijken. Hier geldt één uitzondering op. Specifiek voor financiële instellingen wordt voor de verbodsbepalingen onder artikel 5, eerste lid, onderdelen a en b, de AFM aangewezen als markttoezichtautoriteit. De AFM houdt momenteel al toezicht op de naleving van wetgeving die moet voorkomen dat consumenten gemanipuleerd of uitgebuit worden door financiële instellingen. Denk bijvoorbeeld aan zorgvuldige dienstverlening, integere bedrijfsvoering, product governance of niet-misleidende informatieverstrekking. Het toezicht op verboden AI-praktijken door financiële instellingen is daar een aanvulling op.

Hoog-risico systemen als veiligheidscomponent in producten

In bijlage I van de verordening zijn twee lijsten met EU-productregelgeving opgenomen. Afdeling A bevat een lijst van EU-harmonisatiewetgeving op basis van het nieuwe wetgevingskader (NWK). De toepasselijke eisen uit de AI-verordening zijn van toepassing indien op grond van die harmonisatiewetgeving een externe conformiteitsbeoordeling vereist is voor deze producten. Afdeling B van deze bijlage valt nog niet onder het NWK van de EU, waardoor de AI-verordening daar niet rechtstreeks op van toepassing kan zijn. Voor afdeling B van bijlage I geldt dat de eisen van de AI-verordening in aanmerking zullen worden genomen in nadere regelgeving van de Europese Commissie over AI in die producten.

De verordening neemt als uitgangspunt dat het toezicht op hoog-risico AI-systemen voor deze producten die wel onder het NWK vallen (bijlage I, afdeling

A), moet worden uitgeoefend door de markttoezichtautoriteiten die nu al op de naleving van de betreffende harmonisatiewetgeving moeten toezien. Dat zijn in Nederland de Nederlandse Voedsel en Warenautoriteit (NVWA), de Nederlandse Arbeidsinspectie (NLA), de Inspectie Leefomgeving en Transport (ILT), de Rijksinspectie Digitale Infrastructuur (RDI) en de Inspectie Gezondheidszorg en Jeugd (IGJ). Om zoveel mogelijk aan te sluiten bij bestaande bevoegdheden en om te voorkomen dat meerdere toezichthouders op hetzelfde product toezicht zullen houden, sluit het kabinet zich aan bij de AI-verordening en worden deze toezichthouders op basis van hun bestaande bevoegdheden aangewezen als markttoezichtautoriteit op bijlage I, afdeling A van de AI-verordening.

Hoog-risico AI producten in EU-regelgeving		Markttoezichtautoriteit
1	Machines	NVWA (consumenten) + NLA (professioneel)
2	Speelgoed	NVWA
3	Pleziervaartuigen en waterscooters	ILT
4	Liften en veiligheidscomponenten van liften	NLA
5	Explosieveilig materieel	NLA
6	Radioapparatuur	RDI
7	Drukapparatuur	NLA
8	Kabelbaaninstallaties	ILT
9	Persoonlijke beschermingsmiddelen	NVWA (consumenten) + NLA (professioneel)
10	Gasinstallaties	NVWA
11	Medische hulpmiddelen	IGJ
12	Medische hulpmiddelen voor in-vitrodiagnostiek	IGJ

Hoog-risico AI-toepassingsgebieden (artikel 6, bijlage III)

In bijlage III van de verordening zijn acht toepassingsgebieden met daarin circa 30 verschillende toepassingen opgenomen, die als hoog-risico worden gekwalificeerd. Voor ieder van die gebieden moet een markttoezichtautoriteit worden aangewezen.

Er is bij de voorgenomen inrichting van het toezicht gekeken naar waar het wenselijk is om bij bestaande expertise en bevoegdheden aan te sluiten. Voor het

toepassingsgebied kritieke infrastructuur is dit het geval en worden de RDI en de ILT als markttoezichtautoriteit aangewezen. Dit geldt ook voor het toezicht op financiële instellingen, waarvoor de AFM en DNB als markttoezichtautoriteiten worden aangewezen. Dit geldt ook voor het toezicht op hoog-risico AI-systemen die worden ontwikkeld en gebruikt ten behoeve van hun deel van de gerechtelijke instanties in de rechtsbedeling, waarvoor de PGHR en de voorzitter van de ABRvS worden aangewezen. De overige toepassingsgebieden van bijlage III vallen niet of slechts gedeeltelijk onder afgebakende domeinen en sectoren waar op dit moment al door een specifieke toezichthouder toezicht op wordt gehouden. Het hiervoor aanwijzen van verschillende sector- of domeinspecifieke toezichthouders zou betekenen dat hun rollen, mandaten en bevoegdheden moeten worden uitgebreid en dat zij ieder nieuwe expertise op het gebied van AI en markttoezicht moeten opbouwen.

In het kader van effectief en efficiënt toezicht, om centrale kennisopbouw te bevorderen en versnippering van het toezicht waar mogelijk te voorkomen, is er daarom voor gekozen om de AP aan te wijzen voor alle overige toepassingsgebieden van bijlage III. Omdat er bij het toezicht ook kennis van de context van het gebruik van het systeem nodig is, liggen samenwerkingsafspraken met de sectorale of domeinspecifieke toezichthouders voor de hand.

Voor toezichttaken op het gebied van rechtshandhaving, migratie-, asiel- en grenstoezichtbeheer en democratische processen stelt de AI-verordening specifieke eisen aan de mate van onafhankelijkheid van de markttoezichtautoriteit. Voor de inrichting van het AI-toezicht in de rechtspraak bepaalt de AI-verordening dat het toezicht geenszins afbreuk mag doen aan de onafhankelijkheid van gerechtelijke instanties of anderszins afbreuk mag doen aan hun activiteiten wanneer zij optreden in hun gerechtelijke hoedanigheid. Met al deze randvoorwaarden is rekening gehouden bij de voorgenomen inrichting van het toezicht.

Toepassingsgebied van bijlage III		Markttoezichtautoriteit
1	Biometrische identificatie, categorisatie en emotieherkenning	AP
2	Kritieke infrastructuur	RDI of ILT (domeinafhankelijk)
3	Onderwijs en beroepsopleidingen	AP
4	Werkgelegenheid, personeelsbeheer en toegang tot zelfstandige arbeid	AP
5(a)	Beoordeling of personen aanmerking komen voor essentiële particuliere en publieke uitkeringen en -diensten	AP
5(b)	Beoordeling kredietwaardigheid of kredietscore	AFM en DNB (financiële diensten) en AP (niet-financiële diensten)
5(c)	Premieberekening bij zorg- en levensverzekeringen	AFM en DNB (financiële diensten) en AP (niet-financiële diensten)

5(d)	Hulpdiensten en triage	AP
6	Rechtshandhaving	AP
7	Migratie, asiel en grenscontrole	AP
8(a)	Rechtsbedeling	PGHR en voorzitter ABRvS
8(b)	Democratische processen	AP

Transparantieverplichtingen

Net als bij de verboden AI-praktijken, zijn de transparantie-eisen domein- en sectoroverstijgend. Daarnaast is er voor het toezicht op deze eisen andere (technische) kennis vereist dan voor het toezicht op hoog risico AI-systemen. Het is daarom wenselijk om het toezicht hierop zo veel mogelijk bij één toezichthouder te beleggen.

Het kabinet is daarom voornemens de AP aan te wijzen als markttoezichtautoriteit op de transparantieverplichtingen. Voor het toezicht op de naleving van deze verplichtingen door financiële instellingen worden DNB en AFM aangewezen als markttoezichtautoriteit, om hiermee zo veel mogelijk aan te sluiten bij het toezicht op de informatieverstrekkingsverplichtingen binnen de financiële markten.

Inrichting AI-testomgeving voor regelgeving in Nederland (NL Sandbox)

De AI-verordening verplicht lidstaten tot het oprichten van ten minste één AI-testomgeving (AI regulatory sandbox) vanaf augustus 2026. Binnen een regulatory sandbox bieden markttoezichtautoriteiten ondersteuning aan aanbieders van AI-systemen die tijdens de ontwikkeling van hun innovatieve product of systeem vragen hebben over hoe zij aan de AI-verordening kunnen voldoen. Dit helpt deze ondernemers om hun product conform de regels op de markt kunnen brengen en voorkomt onnodige regeldruk of vertraging door vragen over de AI-verordening. De uitleg van markttoezichtautoriteiten moet de regels uit de AI-verordening verhelderen, zodat het voor aanbieders makkelijker wordt om hieraan te voldoen. Daarnaast krijgen markttoezichtautoriteiten beter inzicht in innovatieve AI-systemen en de vraagstukken die AI-aanbieders tegenkomen. Markttoezichtautoriteiten stellen zich binnen de sandbox innovatievriendelijk en flexibel op, maar er is geen mogelijkheid om regels buiten werking te stellen. In Nederland zullen de markttoezichtautoriteiten gezamenlijk één multisectorale NL sandbox inrichten om vragen uit alle sectoren en domeinen te kunnen behandelen. Binnen de NL sandbox wordt geen technische infrastructuur of data aangeboden. Toezichthouders richten zich op het bieden van juridisch en technisch advies bij activiteiten die een aanbieder uitvoert om een AI-systeem aan de eisen uit de AI-verordening te laten voldoen en in Europa op de markt te kunnen brengen. In het kader van efficiëntie kan het sandbox-proces gecombineerd worden met de bredere voorlichtingstaken van de markttoezichtautoriteiten.

Aanmeldende autoriteiten en aangemelde instanties

Aanmeldende autoriteiten zijn organisaties die aanvragen beoordelen van instanties die willen optreden als externe beoordelaar (conformiteitsbeoordelingsinstantie (CBI)) van AI-systemen onder de AI-verordening. Aanmeldende autoriteiten beoordelen of de aanvragers voldoen aan de geldende vereisten, melden deze aan bij de Commissie en houden vervolgens toezicht op de aangemelde CBI's (vanaf aanmelding zijn dit aangemelde instanties). Voor de producten die vallen onder de harmonisatiewetgeving die is opgenomen in bijlage I, afdeling A, zijn al aanmeldende autoriteiten aangewezen. Deze aanmeldende autoriteiten zijn veelal een minister, waarbij het werk wordt uitgevoerd door daarvoor aangewezen ambtenaren van een markttoezichtautoriteit. Deze aanmeldende autoriteiten worden ook de aanmeldende autoriteit onder de AI-verordening.

Voor bijlage III moet alleen een aanmeldende autoriteit worden aangewezen voor het toepassingsgebied biometrie. Hiervoor wordt de minister van Economische Zaken aangewezen als aanmeldende autoriteit. Voor het uitvoeren van deze werkzaamheden worden ambtenaren van de RDI aangewezen. Voor alle andere toepassingsgebieden van bijlage III kan volgens de AI-verordening worden volstaan met de eigen beoordeling door de aanbieder van het hoog-risico AI-systeem en hoeven daarom geen CBI's te worden aangewezen.

Productregelgeving van bijlage I, afdeling A		Huidige aanmeldende autoriteit
1	Machines	Minister van VWS (consumenten) + Minister van SZW (professioneel)
2	Speelgoed	Minister van VWS
3	Pleziervaartuigen en waterscooters	Minister van IenW
4	Liften en veiligheidscomponenten van liften	Minister van SZW
5	Explosieveilig materieel	Minister van SZW
6	Radioapparatuur	Minister van EZ
7	Drukapparatuur	Minister van SZW
8	Kabelbaaninstallaties	Minister van IenW
9	Persoonlijke beschermingsmiddelen	Minister van VWS (consumenten) + Minister van SZW (professioneel)
10	Gasinstallaties	Minister van VWS

11	Medische hulpmiddelen	Minister van VWS
12	Medische hulpmiddelen voor in-vitrodiagnostiek	Minister van VWS
Toepassingsgebieden in bijlage III		Aanmeldende autoriteit
1	Biometrie	Minister van EZ
2-8	Overige toepassingsgebieden	Eigen beoordeling door de aanbieder van het hoog-risico AI-systeem

Grondrechtenautoriteiten

Wie in Nederland grondrechtenautoriteit is vloeit voort uit artikel 77 van de AI-verordening en de regelgeving op grond waarvan deze nationale overheidsinstanties of -organen bevoegd zijn toe te zien op de naleving van de bescherming van EU-grondrechten. In Nederland zijn dit voornamelijk het College voor de Rechten van de Mens (CRM), de AP (vanuit het toezicht op het grondrecht op gegevensbescherming), de Procureur-generaal bij de Hoge Raad (PGHR), de voorzitter van de Afdeling Bestuursrechtspraak Raad van State (ABRvS), het gerechtshof van de Centrale Raad van Beroep (CRvB) en het gerechtshof van het College van Beroep voor het bedrijfsleven (CBB). Iedere lidstaat moet publiceren wie deze grondrechtenautoriteiten zijn en deze lijst actueel houden.²

² Kamerstukken II, 2024/25, 22112, nr. 3979.

Bijlage 2 - Visuele weergave voorgenomen AI-toezichtstelsel



* RDI wordt Centraal Contactpunt voor de AI-verordening.

** AFM en DNB voor financiële instellingen en diensten binnen het hoog-risico gebied kredietwaardigheid en premiestelling, verboden AI-praktijken of transparantie-eisen.

MAKING THE GENERAL DATA PROTECTION REGULATION MORE EFFECTIVE

KEY MESSAGES

Make the GDPR truly risk-based: The GDPR should truly prioritise real risks over routine low-risk processing, using a proportionate approach that supports innovation, compliance, and respect for fundamental rights and freedoms.

Enable access to data for Artificial Intelligence (AI) and European innovation: Clarify that pseudonymised and low-risk data may be used for R&D and AI development, and reduce the barriers created by today's broad definition of personal data and rigid purpose limitation.

Cut unnecessary administrative burdens: Excessive documentation and reporting obligations consume vast resources, and are unduly and disproportionately costly¹, without improving privacy outcomes.

Make data subject rights compliance workable: Rights remain essential and must be effectively protected. At the same time, their exercise should not be abusive or result in a disproportionate workload. Obligations should be clarified, simplified, and aligned with risk.

Simplify international data transfers: The EU should take more responsibility at systemic level through additional adequacy decisions and clearer guidance, thus reducing the heavy burden now placed on individual companies.

WHAT DOES BUSINESSEUROPE AIM FOR?

Clarity, proportionality, and a cooperative regulatory approach can make the GDPR a source of empowerment rather than a constraint. Grounded in real-world practicality, it can evolve into a framework that truly balances protection and innovation.

¹ According to the 2024 Draghi report on competitiveness, GDPR compliance costs may reach EUR 500,000 for SMEs and EUR 10 million for larger organizations.

CONTEXT

Europe has successfully raised the bar on data protection, embedding respect for personal data across the economy. Companies of all sizes have been investing, adapting, and acting in good faith to comply. Yet while awareness is strong, practical consistency and maturity in implementation are still evolving².

Legal uncertainty and fragmented enforcement slow innovation. The combination of differing interpretations, complex compliance requirements, and the threat of heavy sanctions creates hesitation rather than rejection of the rules among businesses. Data protection and the freedom to conduct business are not competing goals, but the perception that efforts in compliance are never enough can inadvertently discourage innovation and limit Europe's digital competitiveness³.

Action is needed for clarity, and coherence. Moving from fragmentation to alignment among national Data Protection Authorities (DPAs), the European Data Protection Board (EDPB), businesses and citizens will reinforce trust and unlock innovation.

The proposed Digital Omnibus changes related to the General Data Protection Regulation represent a meaningful step in the right direction. Below, we share views broadly aligned with the approaches recently proposed by the Commission, and offering some suggestions for improvement.

DEFINITION OF PERSONAL DATA AND RISK-BASED APPROACH (ARTICLES 4.1; 5, 24, 33, 34 AND RECITALS, 24, 26)

The broad scope creates disproportionate burdens, and hinders innovation since the definition, legal bases, and purpose limitation taken together significantly restrict collection, sharing and use of data. A clarification should also address the legal status of pseudonymised and anonymised data, reflecting the Court of Justice of the EU (CJEU) reasoning in Case C-413/23 P that whether a person is identifiable depends on the processing context, the means reasonably likely to be used by the data recipient rather than only by the controller, and the actual risk of re-identification.

Strengthening the risk-based approach for data processing is essential to reduce the burden on businesses. Accountability obligations, like documentation and organisational measures, and reporting obligations for low-risk and mundane processing activities may be excessive in relation to the context and potential risk to data subject's rights.

Moreover, principles of data protection require modernisation to reflect technological developments and contemporary data processing methods: particularly, purpose limitation, storage limitation, data minimisation, and the unlimited accountability of the controller, which increasingly conflict with large-scale data processing and AI-driven operations.

² The Fundamental Rights Agency (2024; 2020) notes that awareness of data protection rights does not necessarily translate into understanding, as evidenced by the high number of "trivial or unfounded" and "petty and repetitive" complaints received by Data Protection Authorities.

³ Regulatory complexity, legal uncertainty, and compliance risk are identified in the Draghi competitiveness report as factors that can weaken innovation incentives, particularly for smaller firms. Supporting [evidence from Finland](#) shows that GDPR implementation reduced pharmaceutical and biotechnology R&D spending by up to 39 percent within four years, with the strongest effects among firms operating exclusively under the EU regulatory regime. Consistently, the European Innovation Scoreboard identifies a share of firms with no inclination to innovate.

SUGGESTED IMPROVEMENTS:

- Clarify the use of pseudonymised/anonymised data as to when it can be treated as non-personal data in line with the CJEU Case C-413/23 P, in Article 4 and consistently in Recital 26 by establishing an approach based on the entity processing the data and the means it actually has at its disposal.
- Article 5 must reaffirm the risk-based nature of the Regulation and its balance of data protection and innovation in the economy, with a corresponding reflection in Article 24. Further processing for archiving, research⁴, statistical, or public-interest purposes should be explicitly treated as automatically compatible, removing the need for a separate Article 6(4) assessment, which often adds unnecessary red tape. This ensures efficiency while keeping all Article 89(1) safeguards in place to protect data subjects' rights.
- An adaptation of the applicable requirements according to the level of risk would also enhance overall coherence with the AI Act, which clearly differentiates the obligations applicable to an AI system based on the level of risk associated with it.
- Heighten the threshold for data breach reporting, so only high-risk breaches are covered, and consider merging Articles 33 and 34. Such an evolution would help avoid excessive notification of minor incidents, which provide limited value for supervisory authorities, while allowing resources to be focused on significant risks.

E-PRIVACY DIRECTIVE AND THE GDPR

Aligning parts of the e-Privacy Directive with the GDPR would be beneficial for the recognition that certain uses of data can help service providers to improve and maintain quality without unnecessarily burdening users with frequent consent requests. Such framework would continue to safeguard personal data, while offering a clear, structured approach for responsible data use.

- Move the “cookie rule” from the ePrivacy Directive to the risk-based framework of GDPR, or “whitelist” low-risk, essential activities (e.g., security monitoring, software updates, anti-fraud, and first-party analytics).

CLARITY ON LAWFUL BASIS FOR PROCESSING (ARTICLES 6 AND 9)

Lawfulness of data processing activities has been a point of tension over the years. Subsequent legal acts in the digital sphere have treated different legal bases as to clarify which one is more suitable for particular activity, thus creating confusion as to whether the legal bases are ranked or not. In addition, certainty is necessary, especially for further processing for example for AI training, or other emerging technology developments.

SUGGESTED IMPROVEMENTS:

- Clarify in the GDPR that companies have a clear legal basis in Article 6, such as legitimate interest; research grounds, for training AI models and systems.

⁴ Including one that would support innovation, technological development, and R&D activities of the private sector. The GDPR Recital 33 allows for broader consent of certain areas of scientific research. Business R&D often uses the same methodologies, experimentation, and has contributed to major breakthroughs, and should also more explicitly benefit from such broader consent.

- Reaffirm “legitimate interest” for AI training and clarify rules to ease the processing of data that has been manifestly made public by individuals.
- Reflection in Article 9 on balanced processing of special categories of data in line with technological developments, such as AI, would be necessary, for example by introducing carefully scoped exceptions that allow use of sensitive data for AI, while underpinning safeguards to protect individuals’ rights. This approach would balance technological progress with fundamental data protection principles.

DATA SUBJECT RIGHTS: PRACTICAL CHALLENGES AND MISUSE (ARTICLES 12 TO 15)

Data subject rights are often perceived as absolute, and not as relative to other persons rights, freedoms and legal obligations. This creates unrealistic expectations, especially regarding access and erasure, or rejection of request. The scope of uncertainty on what must be disclosed is high. Identification challenges to verify data subjects’ requests persist. Yet, any non-compliance by business is portrayed as intentional, which fuels negative perceptions, and discourages engagement, particularly among SMEs.

Data subject requests are a large administrative burden, time-consuming and costly. Moreover, the volume of data subject rights requests has been increasing significantly each year, to the point of becoming difficult to manage for many organisations, particularly for SMEs, which often lack the resources to handle such requests effectively. This imbalance led to the misuse of data protection rights for purposes unrelated to safeguarding personal data, exposing controllers to heightened legal and reputational risks. A growing risk of misuse of these rights can thus be observed, where they are used: (i) as leverage in litigation to obtain evidence, for instance in employment disputes; (ii) as a means of exerting pressure on companies through repeated or coordinated requests from activists; or (iii) as a reputational or image-related tool without any direct connection to the genuine protection of personal data.

SUGGESTED IMPROVEMENTS:

- Clarify that the rights are not absolute, especially to avoid intrusive monitoring obligations and ensure the balance with other persons’ rights.
- The possibility to reject a request on grounds that its purpose is abusive (e.g., manifestly unfounded or excessive, especially if the request is made for purpose other than data protection) can be considered. Data subjects must cooperate in this process of clarifying the purpose of the request.⁵
- Unfounded, abusive, misused, and excessive requests should be further defined in guidelines issued by the European Data Protection Board (EDPB).
- Consider less information obligations under Articles 13–15 where more proportionality is needed.

⁵ Suggestion, Article 12 (5): Information supplied under Articles 13 and 14, as well as any communications or measures taken under Articles 15 to 22 and 34, must be provided to the data subject at no cost. However, if a request cannot reasonably be met, is clearly unfounded or excessive, particularly when repeated, or would require a disproportionate effort in light of the actual risk or alleged harm, the controller may either charge an appropriate fee reflecting the administrative effort needed to provide the requested information, communication, or action, or refuse to comply with the request after asking the data subject to clarify the purpose and the specific processing activities concerned.

AUTOMATED DECISION-MAKING (ARTICLE 22)

The application of Article 22 GDPR regarding automated decision-making is often interpreted narrowly. Some data protection authorities claim that automated decisions cannot be considered “necessary” simply because humans have historically performed such tasks. They draw the conclusion that automated decision-making is not permissible and that an effective consent according to Article 22(2)(c) and Article 7(4) can only be given if the data subject has the opportunity

to choose processing by a human being from the beginning. However, such a narrow interpretation of what can be considered necessary would prevent businesses and consumers from fully accessing the benefits new technology. This restrictive reading often prevents digital solutions, such as online contracts or automated tasks processing (i.e., automated claims processing).

SUGGESTED IMPROVEMENTS:

- GDPR’s Article 22 should be reformed and aligned so that compliance with the due diligence obligations in the AI Act enables a legally compliant use under GDPR, provided a legitimate interest is pursued.

PRIOR CONSULTATION AND DPIA GUIDANCE (ARTICLES 35 AND 36)

Article 36 requires prior consultation only when a “Data Protection Impact Assessment” DPIA identifies a high risk that cannot be mitigated, and some DPAs interpret their guidance role as limited to these non-mitigatable high-risk cases. This leaves controllers, especially those using highly innovative technologies, facing regulatory uncertainty, and unable to seek support until risks are already severe, leading to delays and uneven compliance. Yet Article 57 makes clear that DPAs must promote awareness of risks, rules, safeguards, and controller obligations more broadly. Such a narrow interpretation does not help with proactive oversight.

Furthermore, current DPIA practices can sometimes become routine “tick-box” exercises, particularly when requirements are rigid or interpreted inconsistently across authorities, which makes it harder for organisations to focus on genuinely high-risk processing.

SUGGESTED IMPROVEMENTS:

- Articles 35 and 36: The DPIAs requirements will also benefit from risk-based clarification, and prior consultation to the supervisory authority on a voluntary basis should be permissible not only for reactive situations, but also, for example, where the results of the impact assessment are not conclusive.
- Streamlining DPIA requirements and harmonising templates would also help reduce complexity of internal processes and cut administrative burden for businesses.

INTERNATIONAL DATA TRANSFERS (ARTICLES 44 - 47)

International data transfers have not been smooth, especially for smaller players. The conclusion of adequacy decisions with different jurisdiction has not been at the speed that would allow scale and certainty for expanding business operations abroad.

SUGGESTED IMPROVEMENTS:

- A thorough assessment of the international data transfers challenges under the GDPR must be conducted, and the process reformed.
- Clarify that the risk-based approach (Articles 24 and 32) applies also to the measures for data transfers to third countries (Chapter V).
- Simplify the validation process of Binding Corporate Rules (Article 47).
- Create a positive presumption for intra-group transfers where a group self-certifies adherence to appropriate safeguards. Assessment of a third country's laws should focus on the actual likelihood of public authorities accessing EU persons' data.

REGULATORY COOPERATION AND PROCEDURAL CERTAINTY (ARTICLES 51 - 57)

The Helsinki Commitments already outline valuable principles for transparency, stakeholder engagement, and predictability in European Data Protection Board (EDPB) and national data protection authorities (DPAs) cooperation. To ensure these remain stable and consistently applied over time, it would be helpful to explore whether some procedural guarantees, such as clearer consultation practices, feasibility assessments, transparency, could be reflected at the legislative level. This would strengthen trust, reduce uncertainty for stakeholders, and ensure continuity of the practice.

SUGGESTED IMPROVEMENTS:

- The process of EDPB guidelines could be amended to include feasibility checks ahead of adoption, engage stakeholders from the beginning, and include transparency requirements on how stakeholders' input has been treated (the Helsinki statement).
- Article 57 should more clearly state that DPAs have a responsibility to guide controllers and processors on data processing activities beyond only non-mitigatable high-risk cases, reinforcing cooperation and strengthening the
- protection of data subjects.
- The principle of proportionality, already stated in recitals, must be made explicit in the main text to guide enforcement by DPAs.

BUSINESSEUROPE



BusinessEurope is the leading advocate for growth and competitiveness at the European level, standing up for companies across the continent and campaigning on the issues that most influence their performance. A recognised social partner, we speak for enterprises of all sizes in 36 European countries whose national business federations are our direct members.



Austria



Belgium



Bulgaria



Croatia



Cyprus



Czech Republic



Denmark



Denmark



Estonia



Finland



France



Germany



Germany



Greece



Hungary



Iceland



Iceland



Ireland



Italy



Latvia



Lithuania



Luxembourg



Malta



Montenegro



Norway



Poland



Portugal



Rep. of San 5.1.2.e



Romania



Serbia



Slovak Republic



Slovenia



Spain



Sweden



Switzerland



Switzerland



The Netherlands



Türkiye



Türkiye



Ukraine



Ukraine



United Kingdom



Avenue de Cortenbergh 168
B - 1000 Brussels, Belgium
Tel: +32(0)22376511 / Fax: +32(0)22311445
E-mail: main@businesseurope.eu

WWW.BUSINESSEUROPE.EU

EU Transparency Register 3978240953-79

Gespreksnotitie Regeldruk Omnibusmethode en Omnibus Digitaal/AI

Gesprek College ATR met Eerste Kamer-rapporteurs voor de Omnibus Digitaal/AI, 13 mei 2026.

Inleiding

De Eerste Kamer heeft het Adviescollege toetsing regeldruk (ATR) gevraagd om te delen hoe het college aankijkt tegen de Omnibus Digitaal/AI. De voorliggende notitie bevat de opvattingen van het college over het genoemde omnibuspakket. De invalshoek die het college hierbij hanteert, is dat een goede kwaliteit van wetgeving vraagt om goed onderbouwde politieke besluitvorming. Voor wat betreft Europese regelgeving heeft ATR twee taakopdrachten. De eerste is dat het beoordeelt of BNC-fiches een adequaat beeld geven van de regeldrukeffecten van voorstellen van de Europese Commissie voor specifiek Nederland. De tweede taak is om te adviseren over wetgeving waarmee Europese regelgeving in Nederland wordt geïmplementeerd. Daarbij komt met name ook het vraagstuk aan de orde of die implementatie lastenluw plaatsvindt (d.w.z. zonder onnodige regeldruk). Verder is in dit verband relevant dat ATR via het netwerk van gelijkaardige Europese instanties (genaamd RegWatchEurope) in het Europese domein optreedt, met name door ongevraagde adviezen aan de Europese Commissie over Better Regulation-onderwerpen.

In deze notitie schetst het college kort wat het ziet als de belangrijkste aspecten van de Omnibusmethode. Het college merkt daarbij op dat veel van de bevindingen in deze notitie ook relevant zijn voor voorstellen voor Europese regelgeving in bredere zin.

Omnibusmethode

In 2025 zijn tien Omnibuspakketten verschenen. Met deze pakketten is volgens de Commissie zelf naar verwachting een regeldrukreductie van € 11,9 miljard gemoeid. Ook voor 2026 zijn nieuwe Omnibuspakketten aangekondigd.

De Omnibusmethode kenmerkt zich door:

- *Bundeling* van wetgeving waar lastenreducties mogelijk zijn. Binnen een pakket vertoont die wetgeving enige maar geen strikte samenhang.
- *Snelheid*. De medewetgevers (Raad van de EU en Europees Parlement) worden gevraagd om hun processen aanmerkelijk te versnellen. Onderdeel van die versnelling is de opzet van de hiervoor opgerichte 'Antici Group on Simplification' (een voorportaal van COREPER II) waarin het zwaartepunt bij generalisten in plaats van zaakdeskundigen is gelegd.
- *Vergroting speelveld*. Ook recente wetgeving die pas net is aangenomen of net in werking is getreden, kan binnen een Omnibus worden aangepakt. Een voorbeeld is Omnibus 1 over duurzaamheidsverslaggeving. Ook komt het voor dat wetgeving via een Omnibus werd herzien terwijl er volgens de normale wetgevingskalender al op korte termijn een evaluatie en een normale herziening was gepland. Dit geldt bijvoorbeeld voor Omnibus 3 over Gemeenschappelijk Landbouwbeleid.
- *Urgentie*. Het gebruik van de Omnibusmethode wordt veelal onderbouwd onder verwijzing naar de urgentie van het verbeteren van de concurrentiepositie van Europese bedrijven,

mede in het licht van de diagnose in het Draghi-rapport. Of een dergelijke politieke urgentie deze aanpak werkelijk rechtvaardigen kan, is een vraag die voor veel discussie heeft gezorgd. Met de herijking van het Better Regulation-kader (zie hierna) is de Commissie aan deze kritiek tegemoetgekomen door strengere eisen aan het urgentie-criterium te stellen.

- *Tijdsconsistentie van beleid.* De Commissie geeft bij elk Omnibuspakket aan dat de doelen van de wetgeving in kwestie overeind blijven. De lasten die worden gereduceerd, worden als *onnodig* en/of *disproportioneel* gezien. De Omnibuspakketten vormen daarmee een correctie op lasten die bij eerdere besluitvorming niet als zodanig werden beschouwd. Dit is op zich een heldere doelstelling. Kanttekening bij de vereenvoudigingen is wel dat frequente beleidswijzigingen zelf een bron van regeldruk kunnen vormen, omdat ze gepaard kunnen gaan met desinvesteringen voor bedrijven die al hebben geïnvesteerd in *compliance*. Deze desinvesteringen betekenen niet dat de onnodige of disproportionele lasten niet moeten worden verminderd. Ze beperken wel de (netto-)vermindering van de lasten in de praktijk en kunnen ook leiden tot ervaren regeldruk (als gevolg van het steeds moeten aanpassen aan veranderende verplichtingen).

Vanuit Better Regulation-perspectief heeft de Omnibusmethode een aantal gevolgen:

- Er worden geen volwaardige Impact Assessments gemaakt maar volstaan wordt met begeleidende Memo's (hierna: Staff Working Documents of *SWDs*). De *SWDs* beperken zich tot het volgende:
 - o Weergave van de klachten die v.w.b. de betreffende wetgeving zijn binnengekomen. Het is niet altijd goed mogelijk om de klachten te herleiden tot specifieke consultaties.
 - o Kwalitatieve weergave van regeldruk-reductiepotentieel volgens de Commissie.
 - o Berekening van de kostenreductie. Deze berekeningen laten veel lacunes zien.
- Er vindt een lossere omgang plaats met consultatie.
- De Commissie-interne kwaliteitstoetsing versobert. Zo moest bij Omnibus I over duurzaamheidsverslaggeving een interne check binnen 24 uur plaatsvinden (vallend in het weekend).
- De onafhankelijke toetsing wordt beperkt. De Regulatory Scrutiny Board (RSB) heeft als belangrijkste rol het adviseren over impact assessments. Zonder impact assessments heeft de RSB dus geen formele adviesrol meer met betrekking tot de kwaliteit van de onderbouwing van een Omnibuspakket.
- Ook de termijnen voor behandeling en t.z.t. voor omzetting/implementatie worden ingekort.

Bevinding 1:

Het voorgaande betekent dat de Omnibusmethode leidt tot minder strikte checks and balances en tot een beperktere kwaliteitstoetsing.

Omnibusmethode heeft potentie en risico's

Nederland heeft zich steeds kritisch getoond op de Omnibusmethode, maar is er tot op heden wel in meegegaan. In discussies met de Eerste Kamer (Verslag Schriftelijk overleg 13 maart 2026) komt naar voren dat het kabinet wellicht concrete consequenties gaat trekken uit de kritische houding. In een concept non-paper dat het kabinet op 8 april jl. aan de Eerste Kamer heeft gestuurd en dat aan de Europese Commissie en de Lidstaten zal worden aangeboden,

wordt van wijzigingsvoorstellen voor met name de AVG gesteld dat zij te fundamenteel zijn om in een Omnibusproces af te handelen.

Vanuit het perspectief van Better Regulation is een eerste opmerking dat de Omnibusmethode veel potentie heeft om onnodige regeldruk tegen te gaan. De methode past bij de Nederlandse ervaring dat veel regeldruk een Europese oorsprong heeft. Cruciaal daarbij is dat de methode aan de wetgever het inzicht moet bieden welke verplichtingen tot hoeveel regeldruk leiden en in welke mate ze daadwerkelijk bijdragen aan het voorkomen/oplossen/verminderen van een maatschappelijk probleem. Alleen met dit inzicht kan de wetgever de politieke weging van belangen en gevolgen maken.

Vanuit Better Regulation-perspectief kan worden opgemerkt dat de Omnibusmethode minder zorgvuldig is dan de reguliere Europese wetgevingstrajecten, vooral omdat zij niet gebruik maakt van uitgebreide impact assessments. Daar passen twee kanttekeningen bij. De eerste is dat in de praktijk lang niet alle voorstellen van de Europese Commissie vergezeld gaan van een (uitgebreid) impact assessment. De werkwijze die de Commissie hanteert bij het onderbouwen van wetsvoorstellen, wordt internationaal als 'best practice' gezien, maar in de praktijk blijkt dat de Commissie lang niet altijd deze werkwijze volgde.

De tweede kanttekening is dat er een groot verschil kan zitten tussen de door de Commissie berekende regeldrukgevolgen en de omvang van die gevolgen in de praktijk. Europese kostencalculaties zijn soms substantieel lager. Een voorbeeld hiervan is de Corporate Sustainability Reporting Directive (CSRD), waar RegWatchEurope een [Position Paper](#) over heeft uitgebracht dat ook ingaat op het eerste Omnibuspakket. De Deense regering becijferde bijvoorbeeld dat de werkelijke lasten van de CSRD in Denemarken vijfmaal hoger uit zouden vallen dan door het Impact Assessment voorzien.

Gelet op het feit dat veel regeldruk in Nederland een Europese oorsprong kent, is het belangrijk dat de Omnibuspakketten (de beoogde vermindering van) de regeldruk goed in beeld brengen. Een korte analyse van de BNC-fiches voor deze pakketten leert dat geen van deze fiches een doorvertaling van de Europese regeldrukbedragen naar de Nederlandse situatie bevat. Wel hebben sommige fiches kwalitatieve duidingen die relevant zijn vanuit twee andere toetsingsmaatstaven die ATR hanteert, namelijk 'werkbaarheid' en 'consequenties vanuit uitvoering, handhaving en toezicht'. Zo stelt bijvoorbeeld het fiche bij de Omnibus over het Gemeenschappelijk Landbouwbeleid vast dat sommige vereenvoudigingen in strijd lijken te zijn met de (eveneens Europese) waterkwaliteitseisen, zonder dat de Commissie hieraan gedacht lijkt te hebben. Dergelijke tegenstrijdigheden zijn van belang omdat ze betekenen dat de beoogde vermindering van de regeldruk niet zal worden verwezenlijkt. Ook relevant in deze is dat bij het in beeld brengen van de regeldrukgevolgen rekening moet worden gehouden met aanpassingskosten bij het bedrijfsleven. Het gaat daarbij niet alleen om de investeringen die bedrijven moeten doen om aan nieuwe verplichtingen te voldoen, maar ook om de desinvesteringen die het gevolg zijn van de wijzigingen in het beleid. Die desinvesteringen betekenen dat de door de Omnibuspakketten veroorzaakte regeldrukreducties minder groot zullen zijn.

Bevinding 2:

Vanuit het perspectief van het tegengaan van onnodige regeldruk constateert het college dat de Omnibusmethode het gevaar met zich meebrengt dat de gevolgen van Europese regelgeving niet transparant zijn. Dit kan goed onderbouwde besluitvorming in de weg staan. De Omnibusmethode kan behulpzaam zijn bij het wegnemen van als onnodig of disproportioneel beschouwde verplichtingen, maar dergelijke vereenvoudigingsmaatregelen

vergen wel inzicht in hun effecten. Dit inzicht is met name nodig voor het vertalen ervan naar de Nederlandse context.

Mededeling 'A Simpler, Clearer and Better Enforced EU Rulebook'

Op 28 april jl. heeft de Europese Commissie een mededeling over het Better Regulation-kader gepubliceerd. De achtergrond hiervan is dat de kwaliteitseisen voor wetgeving door de Commissie zelf als zwaar en belastend worden ervaren. Vergeleken met de praktijk in veel Lidstaten is dit een terechte constatering. Tegelijkertijd moet ervoor worden gezorgd dat de onderbouwing van voorstellen van de Europese Commissie voldoende blijft.¹ De bedoeling van de herziening is onder andere om meer flexibiliteit in te bouwen.

In de Mededeling geeft de Commissie aan dat veel meer wetgevingsvoorstellen van een impact assessment zullen worden voorzien. Dit betekent dat het urgentie-criterium voor toekomstige Omnibus-voorstellen zeer waarschijnlijk niet meer zal worden gebruikt, en deze praktijk dus niet meer buiten de kaders voor kwaliteit van regelgeving zullen vallen. Om meer voorstellen van een 'normaal' impact assessment te voorzien en tegelijkertijd het wetgevingsproces sneller en eenvoudiger te maken, is het nodig om dit 'normaal' opnieuw te definiëren. Een belangrijk aspect is om impact assessments soberder te maken. Ze waren namelijk uitgegroeid tot zeer omvangrijke documenten met weinig focus. Door vaker impact assessments over meer wetgevingsvoorstellen te maken krijgt ook de Regulatory Scrutiny Board weer een grotere adviesrol. Wel wordt de impact van zijn oordelen bij kleinere voorstellen ('targeted proposals') terugschroefd tot het doen van aanbevelingen.

Voor bestaande wetgeving is een 'Regulatory Deep Cleaning Action Plan' in werking gesteld. Onderdeel daarvan is een nieuw opgerichte Simplification Platform waar alle relevante groepen belanghebbenden zitting in hebben. Er zijn 12 focusgebieden aangewezen waar tot aan het einde van 2027 vereenvoudigingen zullen worden onderzocht en geïnitieerd. Het digitale domein is een van die focusgebieden. De al lopende Digital Fitness Check is een belangrijk vehikel om potentiële vereenvoudigingen op het spoor te komen. Een Fitness Check is een beleidsterrein-overschrijdende ex-post analyse, die met name overlap en complexiteit aan het licht moet brengen.

De Mededeling bevat verder voornemens die moeten leiden tot eenvoudiger en begrijpelijker wetgeving. Zij kondigt aan dat scherper wordt gelet op nationale koppen (ook als die Europeesrechtelijk zijn toegestaan), en strenger wordt opgetreden tegen te late of onjuiste implementatie.

Bevinding 3:

Het is positief dat meer wetgevingstrajecten onder de normale kwaliteitscriteria worden gebracht. Het college acht het legitiem dat Commissie meer flexibiliteit heeft ingebouwd in het Better Regulation-kader. Belangrijk gevolg daarvan is namelijk dat er minder buiten dat kader zal worden geplaatst vanwege politieke urgentie. Ook de aanwijzing van 12 focusgebieden waar als eerste stap het vereenvoudigingspotentieel rigoureus en navolgbaar zal worden onderzocht, is positief. Dit biedt Nederland de kans om deze gebieden ook te analyseren, en inbreng te leveren in een vroege fase van het Europese proces. Het tegengaan van nationale koppen (in de zin van niet-lastenluwe implementatie) ligt in lijn van het kabinetsbeleid in deze.

¹ De Europese Ombudsman heeft het proces van Omnibuspakket nummer 1 (over duurzaamheids-verslaggeving) als onbehoorlijk bestuur aangemerkt. Een van de redenen daarvoor was dat onvoldoende duidelijk werd gemaakt hoe alle relevante belangen zijn betrokken en afgewogen.

Daarvoor is wel nodig dat de regeldrukgevolgen van Europese opt-outs en derogaties – die vaak pas in het onderhandelingsproces worden ingebracht – goed in beeld zijn én worden doorvertaald naar de Nederlandse situatie.

Concrete aandachtspunten Omnibus Digitaal/AI

In het voorgaande zijn aandachtspunten voor de Omnibusmethode in algemene zin besproken. Daarnaast zijn er (vanuit regeldrukperspectief) ook aandachtspunten voor specifiek de Omnibus Digitaal/AI:

- *De verwachte besparingen komen vooral door de vereenvoudiging van de cookie-wetgeving.* De overige bedragen die worden genoemd, zijn kleiner. Het kabinet heeft (in het eerdergenoemde non-paper) mede daaruit de conclusie getrokken dat de besparingen voor wat betreft de AVG beperkt zijn. Dat is voor het kabinet een reden om de meer fundamentele wijzigingen uit het voorstel te schrappen en op een later moment van een gedegener behandeling te voorzien. Een dergelijke behandeling is vanuit regeldrukperspectief overigens wel nodig, gelet op de ervaring dat de praktische (regeldruk)gevolgen van de AVG veel groter lijken te zijn dan oorspronkelijk door de Commissie berekend.
- *Het SWD laat bij veel wijzigingen na om een regeldrukcalculatie te geven* omdat dit niet mogelijk zou zijn wegens onvoldoende data. RegWatchEurope heeft eerder al aangegeven dat het de voorkeur verdient om een bandbreedte te geven in plaats van een post helemaal open te laten. Dit sluit ook aan bij het Nederlandse streven om in dergelijke gevallen te werken met scenario's en/of bandbreedtes. Een dergelijke werkwijze zou ook voor de Omnibus Digitaal/AI behulpzaam kunnen zijn.
- *Doorvertaling gevolgen in BNC-fiches:* De ervaring met betrekking tot BNC-fiches leert dat deze de vermindering van de regeldruk die op Europees niveau is genoemd, tot nog toe niet doorvertalen naar de Nederlandse situatie. Dit geldt ook voor het fiche over de Omnibus Digitaal/AI. Het fiche benoemt wel diverse punten (ook voor wat betreft de kwantificatie) waarbij de Commissie om opheldering zal worden gevraagd.
- *Veel regeldruk ten aanzien van de 'Digital rulebook' (het geheel van EU-regulering van het digitale domein) vindt zijn oorsprong in een gebrek aan houvast voor bedrijven en burgers.* Er is (ook volgens de Commissie) nog een wereld te winnen op het gebied van handleidingen, beleidsregels, uniforme handhaving, 'codes of conduct' en dergelijke. In het kader van de AI Act is het zelfs nog niet gelukt om standaarden vast te stellen. De AVG is al bijna 8 jaar integraal van toepassing, maar daar speelt dit probleem nog steeds. Een gebrek aan houvast en 'guidance' wordt al vanaf het begin signaleerd.
- *De relatief magere onderbouwing van de Omnibus leidt tot markante verschillen in inschatting tussen de Commissie en het Nederlandse kabinet.* Zo wordt de *Platform to Business Regulation* (P2B; EU 2019/1150) door de Commissie als geheel overbodig beschouwd vanwege recentere interventies zoals de *Digital Markets Act* en de *Digital Services Act*, terwijl het kabinet aangeeft dit nog steeds een nuttig kader te vinden waarover weinig klachten vernomen zijn. Voor een appreciatie van beide posities is meer inzicht nodig in de meerwaarde van de P2B Verordening ten opzichte van de genoemde interventies.
- *De Omnibus Digitaal lijkt inderdaad te leiden tot minder (ervaren) regeldruk.* Zij consolideert een aantal eerdere interventies op het gebied van open data in een enkele Data Act. Daarbij worden verplichtingen gestroomlijnd en doublures geschrapt.

- *De wijzigingen in de AI Act lijken niet tot veel desinvesteringen te leiden.* Het gaat voornamelijk om de beslissing om de bindende inwerkingtreding uit te stellen in het licht van de tegenvallende voortgang van het ondersteunende beleid. De scope wordt niet veranderd. Wel zijn er een aantal principiële wijzigingen (met beperkte regeldrukgevolgen) in de AVG voorgesteld t.a.v. het trainen van AI-modellen. Deze zijn door het kabinet aangemerkt als te fundamenteel om in een vereenvoudigingspakket te kunnen worden behandeld.
- *Raad en Parlement brengen gevolgen wijzigingen niet in beeld:* Een voorgestelde vermindering van regeldruk komt voort uit het schrappen van een verplichting die door een amendement in de AI Act terecht is gekomen en waarvoor nooit een impact assessment was gemaakt. Dit is de verplichting voor bedrijven om de AI-geletterdheid van werknemers te waarborgen. Een veelgehoorde klacht was dat het voor bedrijven onduidelijk was wanneer zij hieraan voldoen. Het feit dat voor dit amendement nooit de effecten in beeld zijn gebracht, vindt zijn oorsprong in de niet-naleving door de Raad en het Parlement van de toezegging in het Interinstitutioneel Akkoord Betere Regelgeving om bij substantiële amendementen ook de effecten in kaart te brengen. Dit probleem wordt al jaren gesignaleerd, maar ondanks de inspanningen van recentelijk het Poolse en Deense voorzitterschap zijn er nog steeds geen vorderingen te melden. RegWatchEurope heeft in het eerdergenoemde *Position Paper* in bredere zin aandacht gevraagd voor het feit dat EU Impact Assessments niet actueel worden gehouden, maar desondanks wel als referentie dienen in de Lidstaten.
- *Impact assessments onderschatten de daadwerkelijke kosten:* In Omnibuspakket nummer 4 over Small Midcaps (een nieuwe categorie van middelgrote bedrijven) werd een wijziging in de AVG voorgesteld die de regeldruk meer beperkt dan hetgeen in de Omnibus Digitaal staat. Dit betrof de verplichting om alle gegevensverwerkingen te registreren en te documenteren, zodat deze bij een eventueel verzoek van de gegevensbeschermingsautoriteit (DPA) beschikbaar zijn. Deze verplichting zou zowel voor het MKB als voor Small Midcaps opgeheven worden. Een binnenkort te verschijnen essay van RegWatchEurope over de kosten van de AVG laat zien dat de kosten van deze verplichting aanvankelijk (in 2012) zwaar onderschat waren.

Bevinding 4:

De verwachte vermindering van de regeldruk in de Omnibus Digitaal/AI komt vooral door wijziging van de cookie-wetgeving. Van veel wijzigingen zijn de regeldrukgevolgen echter niet duidelijk, noch op Europees en noch op Nederlands niveau. Het risico is bovendien dat de feitelijke regeldruk zal afwijken van de berekende regeldruk. Dit risico is reëel, gelet op het feit dat de gevolgen van wijzigingen die door Raad en Parlement worden aangebracht, niet in beeld worden gebracht.

Tot besluit

Deze notitie schetst vanuit regeldrukperspectief de belangrijkste aspecten van de Omnibusmethode. In de kern komen deze aspecten erop neer dat ook vereenvoudiging vraagt om een goed beeld van de regeldrukeffecten, omdat alleen dan de wetgever de afweging kan maken of (en in welke mate) verplichtingen leiden tot disproportionele regeldruk. In het verleden lijkt de onderbouwing van Omnibuspakketten aan kwaliteit te hebben ingeboet. Het voornemen van de Commissie om in de toekomst weer impact assessments te maken, ook

van Omnibuspakketten, verdient vanuit regeldrukperspectief ondersteuning. Zorgpunt daarbij is de discrepantie tussen de regeldrukberekeningen van de Commissie enerzijds en anderzijds de uitwerking in de dagelijkse praktijk. Ook leert de (recente) ervaring met de advisering over BNC-fiches dat het moeilijk is om de Europese berekeningen te vertalen naar de specifiek Nederlandse situatie. Dit geldt ook voor wat betreft de Omnibus Digitaal/AI. De kwaliteit van de onderbouwing van dit Omnibuspakket kan verbeteren door in de berekeningen gebruik te maken van scenario's en bandbreedtes. Verder lijkt het zinvol om te werken met 'implementation workshops', waarbij de Commissie en Lidstaten overleggen over goede (lastenluwe) manieren van implementeren. Een tijdige check of de berekende (vermindering van de) regeldruk zich ook in de dagelijkse praktijk manifesteert, is belangrijk om te kunnen bijsturen als de beoogde vermindering niet dreigt te worden gerealiseerd.

DIGITAL FITNESS CHECK – CALL FOR EVIDENCE

Position Paper VNO-NCW and MKB-Nederland

10 March 2026

Public Consultation on the Digital Fitness Check

VNO-NCW and MKB-Nederland welcome the Digital Fitness Check as a step to stress-test the efficiency and effectiveness of the cumulative Digital Rulebook¹. We stress the importance of European legislators to continuously assess, now and in the future, the coherence, clarity, proportionality, enforceability and required implementation efforts of the cumulative rules of the Digital Rulebook to support EU's competitiveness.

Although we can be proud that Europe has set a high level of protection for fundamental rights and consumer safety, it cannot be ignored that the accumulation of the complex rules, the interplay between those rules, the incoherence and unclarity of those rules, the short implementation periods, the unavailability of timely guidance, the diverging interpretations of rules by competent authorities and the gold plating by member states, require disproportionate implementation efforts and resources of companies, specifically smaller companies, which has an adverse effect on competitiveness and hinders technology diversification in the Union.

We concur with the Commission that fast and visible improvements are needed to enable a more cost-effective and innovation-friendly implementation of the rules while maintaining the core objectives of the rules.

¹ EU legislation with a significant digital angle, examples include rules on data, artificial intelligence, telecommunications services, regulations on online platforms and digital services, media services, cybersecurity or privacy of communications.

1. Digital Rulebook – continue simplification efforts

VNO-NCW and MKB-Nederland support the goals of the different rules of the Digital Rulebook and the intention to strengthen legal certainty and a level playing field in the Union. However, the vast and complex digital & data rules of the Digital Rulebook are not yet sufficient coherent, clear, harmonized, predictable, proportionate, and easy to implement. VNO-NCW and MKB-Nederland welcome the earlier simplification efforts of the European Commission² as well as this call for evidence in order to strengthen the legal certainty and proportionality of the Digital Rulebook. These are necessary steps to increase responsible (innovative) development and adoption of AI without lowering the objectives of the Rulebook.

The Digital omnibus and the Omnibus on AI presented by the European Commission on 19th November, are a good first step towards this and we hope more will follow³.

2. EU Digital rulebook – Competitiveness

Acknowledging the importance of boosting competitiveness and innovation in key technologies such as AI and the role of (high quality and pluriform) data within this context while protecting fundamental rights is crucial. The EU's digital rulebook has an important role to play to achieve this. Harmonizing legal digital frameworks in Europe is an essential step to ensure a level playing field in the Union and subsequent strong European businesses.

3. Digital Rulebook - Harmonizing rules is not enough

Harmonizing rules in the Union is key for a strong internal market and a level playing field. However, this is not the sole step that needs to be taken. In addition, making sure digital rules are coherent, clear, predictable, proportionate and easy to implement, is essential. This is necessary to improve legal certainty and the implementation of the rules, which improves trust. For a list of inconsistencies and unclarities in the current Digital Rulebook, we refer to the legal recommendations in the BusinessEurope position papers⁴. This is not an exhaustive list.

Little attention has been paid to the cumulative impact of the rules on

² We refer to our position paper on the Digital Omnibus & Digital Omnibus on AI: <https://www.vno-ncw.nl/brieven-en-commentaren/position-paper-digital-omnibus-and-omnibus-on-ai>

³ We refer to the position papers of BusinessEurope with many examples of inconsistencies, unclarities and overlaps³ which need addressing: Reducing regulatory burden to restore the EU's competitive edge - BusinessEurope (December 2025); Simplifying the EU digital rulebook - a BusinessEurope position paper - BusinessEurope (July 2025)

⁴ The position papers of BusinessEurope with many examples of inconsistencies, unclarities and overlaps⁴ which need addressing: Reducing regulatory burden to restore the EU's competitive edge - BusinessEurope (December 2025); Simplifying the EU digital rulebook - a BusinessEurope position paper - BusinessEurope (July 2025)

business operations and thus on competitiveness. Although we continue to support the policy objectives of the EU Digital Rulebook, applying all these rules together is a considerable challenge for businesses.

Improving coherence and clarity will also limit the room for diverging interpretations by national enforcement authorities. Divergent interpretations hinder a level playing field, hinder investments in innovative technology and deployment of such technologies and fuel a fear to act. A fear to act can make us lose important opportunities which would have benefited society. In addition to their current mandate, give competent authorities/supervisors the legal mandate to take into account European competitiveness, growth and technical diversification. This supports the 'this is how you can do it' mentality instead of solely focusing on risks and communicating how it cannot be done. Emphasize preventive supervision (including implementation tools and practical visualized guidance).

Also, national gold plating needs to be halted to achieve a level playing field, a strong internal market and strong European players. Gold plating leads to fragmentation in the Union which weakens the internal market and hinders doing business, competitiveness, innovation, R&D and adaption of key technologies. Harmonization of rules on EU level will not be sufficient if national MMs continue to gold plate the harmonized acts. We ask the European Commission to take strong action against such gold plating on national level. We agree with the recent remarks of Von der Leyen in which she addressed this problem.

The last essential step, is to refrain from adding new rules unless (a) strong empirical evidence demonstrates a material legal gap; and (b) the purpose cannot be achieved more effectively and efficiently through other measures with less impact on businesses. For instance, by enhancing enforcement. Existing definitions, risk taxonomies, evaluation methods, and standards must also be taken into account, insofar as they exist.

Constructive and timely dialogue with businesses/business organizations and performing reality checks is an essential continuous process. Also, companies must be given sufficient implementation time to properly organize compliance with the rules; business processes cannot be adjusted at the push of a button.

In addition to forementioned better regulation principles, VNO-NCW/MKB-Nederland ask for the following checks to be incorporated in the regulatory process:

- A consistency check. Introduce a check after the trilogue phase to identify and address overlaps, inconsistencies, and contradictions between interacting legislation.
- In the event of substantial amendments, new obligations, or significant expansion of scope introduced during trilogue negotiations a mandatory renewed impact assessment should take place before final adoption.
- A cumulative competition check. Inter-DG assessments of the cumulative impact of new regulatory proposals on the EU's competitiveness, taking into account the interaction of the new rules with other existing and new relevant horizontal and sectoral rules.
- An SME check. Think small: regulations must be reasonably operational for SMEs—also taking into account a possible domino effect—without compromising the intended policy objective.
- Enforcement checks: (a) carry out an enforcement check of existing rules to substantiate the necessity of new legislative proposals. If there are enforcement problems, do not draft new rules but improve enforcement; (b) ensure that enforceability of new EU rules is systematically assessed during legislative impact assessments.
- Break down silos: Create inter-DG task forces for each policy objective so that rules are not developed in silos but, from the outset, there is a clear picture of which existing and other rules the rules to be drafted will interact with and what this means cumulatively for competitiveness and adoptability.
- Realistic reporting and notifications: Limit these to 'realistic must-haves'. They should not only be a means to facilitate possible enforcement actions, but should also offer real strategic added value to contribute to the achievement of the intended policy objective.

4. Overlaps, conflicts, or redundancies between the EU digital legislation and sector-specific EU regulations.

We refer to the position papers of BusinessEurope with many examples of inconsistencies, unclarities and overlaps¹ which need addressing:

- [Reducing regulatory burden to restore the EU's competitive edge - BusinessEurope \(December 2025\);](#)
- [Simplifying the EU digital rulebook - a BusinessEurope position paper - BusinessEurope \(July 2025\)](#)

In addition:

Consumer law - Digital Fairness Act

We are concerned about the introduction of new overlapping, incoherent and disproportionate rules as part of the upcoming Digital Fairness Act.

Specifically, we miss a comprehensive study substantiating the need for a new act. New laws may only be introduced if (a) empirical evidence demonstrates a material legal gap; and (b) the purpose cannot be achieved more effectively and efficiently through other measures with less impact on businesses, such as improving enforcement and/or amending in so far as strictly necessary existing laws (such as the UCPD). An independent study on digital fairness in online retail shows that in almost all cases enforcement authorities already have a legal basis to act:

(<https://www.eurocommerce.eu/app/uploads/2024/11/20240905-kuehling-sauerborn-study-on-digital-fairness-in-online-retail-final-version.pdf>).

However, enforcement is fragmented or insufficient. Introducing new rules where enforcement of existing rules is the appropriate remedy would add complexity without improving consumer protection.

Interplay AI Act and Cyber Resilience Act needs clarification

We miss alignment between the cybersecurity requirements for high-risk AI applications under article 15 AI Act with the cybersecurity requirements under the Cyber Resilience Act (CRA). To prevent overlap and unclarity, we propose to make explicit that an EU Declaration of Conformity under the CRA would demonstrate conformity with article 15 AI Act.

Early termination penalties – Data act

Clarify in the Data Act that received discounts fall within the scope of early termination penalties, for instance discounts received for fixed long term contracts and/or for contracting a combination of different service simultaneously.

Cooperation competent authorities

We opt for the introduction of a legal obligation for competent authorities to

consult with and take into consideration the views of relevant other competent authorities operating in overlapping areas, to coordinate diverging opinions and interpretations of overlapping definitions and obligations and to adopt coherent decisions and guidance that are consistent with applicable interplaying regulation.

Overlap DSA and other digital rules

- DSA & DAC7 overlap (duplicative trader identification requirements)
- DSA & EU Short-Term Rental Regulation (conflicting takedown procedures)
- DSA & AI Act systemic risk assessments (different definitions of risk, separate documentation processes, different supervisory authorities)
- DSA & Payment Services Regulation (PSR) advertising transparency & sector-specific transparency provisions in other regulations
- DSA (dark patterns) & GDPR (consent requirements, transparency, fairness) & UCPD (misleading practices) & Digital Fairness Act (dark patterns, personalization)
- DSA & national illegal-content regimes (different takedown timelines, different procedural channels)
- Introduce a differentiated DSA systemic risk assessment methodology, not limited to platform size (45+ million users) but taking into account the actual risk profile of a service and distinguish between service categories with fundamentally different risk profiles.

5. Examples of national gold plating – Netherlands

The legal conformity period under the Consumer Sale of Goods Directive is two years. However, national divergencies are allowed. In the Netherlands we have a gold plated divergent legal conformity period for products equal to the lifespan of a specific product. This legal conformity period differs per product category and even from product to product within a product category. This leads to uncertainty about the applicable legal conformity period for consumers, traders and producers. This unclarity also causes many discussions between traders and producers about whether a defect falls within or without the legal conformity period of a specific product. In our opinion, it would be more effective and efficient if a harmonized legal conformity period would be in place. This ensures a level playing field and the necessary clarity for all stakeholders.

Another example, concerns the interpretation by competent authorities of the interplay between the Unfair Consumer Practices Directive (UCPD) and the Price Indication Directive (PID). In the Netherlands the market surveillance

authority is of the opinion that setting of a price reduction against the advised price is not allowed under the UCPD, although this is not forbidden under the PID. Again, on EU level it should be made clear that the PID is a *lex specialis* and the UCPD a *lex generalis* and therefore that regarding price indication, the PID trumps the UCPD.

6. Digital Rulebook - governance structure

An enforcement role for the Commission can have clear benefits such as having one enforcer instead of multiple national enforcers in the event of doing business across multiple member states but it needs to be ensured that enforcement mandates are clearly delineated, operationally independent, and subject to robust accountability safeguards to safeguard the trias-politica-principle.

Irvette Tempelman

VNO-NCW/MKB-Nederland

5.2,1

@vnoncw-mkb.nl

19/03/2026

ENSURING EFFECTIVE BURDEN REDUCTION IN THE DIGITAL OMNIBUS

REFLECTIONS ON COMPLIANCE BURDENS, SMES, AND A RISK-BASED APPROACH TO GDPR

With the Council's review of GDPR amendments under the Digital Omnibus underway, and separate discussions ongoing in the European Parliament, it is vital to consider the impact of compliance burdens on enterprises across Europe. Recent signals from the Council's 27 February discussion risk moving in a direction that does not fully reflect the realities of businesses of all sizes.

The Commission's targeted amendments, notably on the definition of personal data and pseudonymised data, provide clarifications grounded in established jurisprudence. These adjustments do not lower protection but make the framework more operational. A relative and risk-based approach ensures pseudonymised data is assessed in context. This avoids disproportionate obligations in low-risk situations and ensures a level playing field in the Single Market.

Clarifications on scientific research follow a similar logic. By confirming a broad understanding of research and removing redundant compatibility assessments, the Commission reduces administrative burdens, especially on smaller organisations, while preserving the safeguards.

A proportionate approach is also needed for automated decision making. Restrictive interpretations risk limiting automation, which has as its very purpose the handling of routine processes efficiently while ensuring appropriate human oversight for critical cases. A clearer framework improves legal certainty, while high-risk applications remain covered by AI Act safeguards.

Removing automated and machine-readable consent from the Digital Omnibus and a thorough, evidence-based review of the ePrivacy framework and its interaction with the amended Article 5(3) is a must. This review should assess legal validity, operational feasibility, enterprise impacts, governance shifts, and sectoral asymmetries before any binding obligations are introduced.

More broadly, while GDPR has made Europe a global standard setter in data protection, it has not yet translated into leadership in data-driven technologies at scale. This invites reflection on whether the framework sufficiently enables companies of all sizes to innovate and grow.

Removing the proposed targeted simplifications would favour those able to absorb regulatory complexity, undermining the Digital Omnibus objective of reducing burdens. Preserving the Commission's approach keeps data-driven innovation open to all European companies, supporting growth, competitiveness, and a vibrant Single Market.



B9+ recommendations for further improvements to the AI Omnibus and the Digital Omnibus

The B9+ Business Federations¹ welcome the European Commission's Digital and AI Omnibus initiatives as an important first step towards regulatory simplification and improved legal certainty. The proposals rightly recognise Europe's competitiveness challenge, marked by excessive paperwork, overlapping obligations and complex rules.

Our vision is a Europe that can access and safeguard the economic benefits of digital transformation, which requires a strong and effective internal market, openness to international cooperation and trade, and a clear focus on competitiveness and resilience. This means creating strong business conditions and building digital capacities across Europe, enabling companies to connect, innovate and trade.

The Omnibus Package is a necessary and promising start for a continuous simplification effort that promotes competitiveness, removes unnecessary administrative requirements, and streamlines AI, data and cybersecurity rules to support compliance and growth. However, EU policy makers must now deliver on this promise.

We welcome the Commission's commitment to further simplification through the Digital Fitness Check, which will be essential to identify inconsistencies, overlaps, and unintended burdens across EU digital legislation. The interplay between any proposed new laws and existing rules must work with, not against, innovation and the goal of EU competitiveness.

Digital Omnibus

The Data Act should ensure genuine protection of trade secrets and security, including explicit coverage of cybersecurity risks arising from data sharing while ensuring uptake of the use of data. An effective dispute settlement mechanism should be available

¹ The D9+ is a Ministerial forum of likeminded and digitally progressive EU Member States. The B9+ Group is a grass-roots coalition of the main national business confederations of 12 D9+ Member States: CEOE (Spain), VBO-FEB (Belgium), SPCR (Czech Republic), DI (Denmark), EE (Estonia), EK (Finland), Ibec (Ireland), FEDIL (Luxembourg), VNO-NCW (Netherlands), LEWIATAN (Poland), CIP (Portugal) and Confederation of Swedish Enterprise (Sweden).

where refusals are considered unjustified, while voluntary data sharing should be facilitated through clearer and more proportionate rules.

Avoid overlaps on **international data transfers**: Provisions on international transfers in the Data Act and DGA should be removed and aligned with existing GDPR rules to reduce complexity. Clarify obligations for mixed datasets and legacy devices to avoid disproportionate or technically impractical requirements. Clarify that the risk-based approach (Art. 24 & Art.32) applies to measures for data transfers to third countries (Chapter V). Create a positive presumption for recognising intra-company transfers during general business when company has self-certified to appropriate safeguards.

The GDPR must be applied in a genuinely risk-based and proportionate manner, focusing on realistic high risks rather than routine low-risk processing. We strongly support the necessary clarification that low-risk processing of personal data requires a less intensive approach than high-risk processing of personal data. This principle of proportionality is made more explicit in the Digital Omnibus proposal regarding the right of access, information requirements and data breach notifications. This is essential to enable access to data for AI and European innovation, including the use of pseudonymised and other low-risk data for innovation and training. We strongly support alignment of Article 4 (definition of personal data) with CJEU case law on sufficient levels of pseudonymisation, and clarification that **legitimate interest** can serve as a legal basis throughout the AI lifecycle, including for security-related processing notwithstanding the other principles and obligations of the GDPR, such as data minimization, purpose limitation etc.

We strongly support the clarification of the definition of **scientific research**. The proposal explicitly confirms that scientific research includes research and technology development (innovation) in academic, industry and other settings such as SMEs. This is the interpretation of scientific research as was initially foreseen by the legislators. The clarification does not alter the requirements for scientific research: research needs to be of high quality and meet the conditions of scientific research, such as methodological and systematic approach.

Unnecessary administrative burdens should be reduced, while data subject rights must remain effectively protected and workable in practice. Legal certainty should be strengthened, including through clearer reliance on legitimate interest for innovation and security purposes, and international data transfers should be simplified through greater EU-level responsibility, a risk-based approach and clearer guidance.

Relevant **parts of the ePrivacy** framework, including Article 5(3), should be integrated into the GDPR, provided the approach is genuinely technology-neutral and risk-based, focusing on processing purposes and real risks rather than specific tools such as cookies. Consent should be reserved for high-risk and highly sensitive processing aligned with the differentiated approach of the GDPR. Broad, undifferentiated consent

requirements dilute meaningful choice and increase “consent fatigue”. A whitelist for low risk essential activities e.g., security monitoring, software updates, anti-fraud and first party analytics (Digital Omnibus, Art. 88a), this is specifically necessary where there is a relationship of authority (such as the employer-employee and government-citizen relationship). Proposed Art 88b introduces economic uncertainty and a new mandatory consent signal on top of existing GDPR rules and should be removed. The proposed browser-level consent mechanism adds complexity without delivering simplification, undermines established publisher-user relationships, and disproportionately harms European SMEs and independent publishers. It risks pushing smaller players behind paywalls, concentrating market power, and restricting low-risk activities such as contextual advertising, fraud prevention, and frequency capping. Co-legislators should instead focus on exempting low-risk activities from consent requirements in line with a risk-based approach.

Other interactions may include between Data Act, DMA, AI Act, DSA and GDPR. Our ask is to identify inconsistencies and overlaps in the Digital rulebook and to ensure these are removed.

Cybersecurity

Deliver a European harmonized secure interoperable technical infrastructure to connect national established Single-Entry Points (SEPs) for reporting that facilitates entities in scope of multiple legal incident reporting obligations to submit one report to be compliant with all applicable rules. See example of Luxembourg and Denmark. We support the setting up of one integrated reporting portal per Member State, covering all statutory reporting obligations, coupled with full EU interoperability through uniform technical and functional standards; and automated and secure transmission where cross-border notifications are required. Companies in all sectors should be allowed to leverage their country of main establishment as the primary interface (single entry point) for cybersecurity incident reporting under relevant EU legislation, provided that this is combined with common templates, definitions and deadlines, and with automated, secure transmission to competent authorities in affected Member States where cross-border notifications are required. ENISA’s role should be supportive and focus on standardisation, interoperability and quality assurance.

Digital Omnibus on AI

High-risk AI obligations should apply **only after relevant harmonised standards, guidelines and key implementation tools are available**, and with sufficient time for adaptation. Also provide sufficient time to ensure that notified bodies² can be formally notified on time to perform the required third party conformity assessments.³ A firm and

² With regard to annex I high risk AI systems

³ Such notification process takes around a year.

realistic application date would be 2 August 2028 to support compliance and avoid fragmented implementation. Similarly, any grace periods on transparency requirements should be realistic and aligned with the delivery of forthcoming Codes of Practice and apply to both providers and deployers.

Regulatory obligations for high-risk AI should be **proportionate and risk-based**, focusing on real risks rather than technology or entire application areas. Unclear delimitation of high-risk AI creates uncertainty and discourages adoption. Reduce administrative requirements for high-risk AI that do not proportionately increase the protection of consumers or society. **Remove or reduce the requirement to register non-high-risk AI systems**⁴. Most systems will not qualify as high risk in practice. This requirement is an administrative burden that impacts innovation/adoption and offers little in terms of risk management or transparency.

Risk assessments and documentation obligations under Articles 5 and 6 should be streamlined. Requirements that do not contribute to effective supervision or risk management should be removed, in line with the objective of reducing administrative burden.

The relationship between the AI Act, the GDPR and sector-specific legislation must be clarified, in particular for high-risk classifications and AI-based safety components. To ensure coherent implementation. High-risk AI requirements should be **integrated into existing sectoral frameworks e.g., Med-Tech**, rather than applied as a parallel regime, allowing standards to align with established compliance systems.

Concluding message

The Digital Omnibus must deliver immediate simplification and legal clarity while laying the foundation for a continuous, evidence-based simplification agenda through the Digital Fitness Check. Only by reducing unnecessary burdens, removing overlaps and ensuring a coherent, risk-based digital rulebook can Europe strengthen its competitiveness, resilience and technological capacity.

⁴ Article 49 of the EU AI Act requires providers to register AI systems in an EU database, regardless of whether they are ultimately classified as high-risk.

Notitie Omnibus AI & Omnibus Digitaal

Het College voor de Rechten van de Mens (hierna: het College) dankt de Eerste Kamer voor de uitnodiging om op 29 april 2026 in gesprek te gaan met de rapporteurs over de Omnibus AI en de Omnibus Digitaal. Voorafgaand aan het gesprek delen wij hierbij onze belangrijkste aandachtspunten met u over de Omnibusvoorstellen. Het College vreest dat de Omnibus AI en de Omnibus Digitaal vergaande negatieve gevolgen voor de bescherming van grondrechten in de Europese Unie kunnen gaan hebben.

Over de Omnibus AI is op 13 maart een compromis in de Raad van de Europese Unie bereikt. Dit Raadscompromis lijkt op sommige punten de voorstellen uit de Omnibus AI te matigen.¹ Nederland heeft zich in de Raad hier ook voor ingezet.² Op 26 maart heeft het Europees Parlement ook haar onderhandelingspositie over de Omnibus AI gepubliceerd, waarin ook een aantal belangrijke matigingsvoorstellen worden gedaan.³ Deze documenten vormen de uitgangspunten voor de trilogonderhandelingen. Omdat de uitkomsten hiervan nog niet vaststaan, bespreken we in deze notitie de belangrijkste aandachtspunten ten aanzien van de bescherming van grondrechten zoals in de oorspronkelijke voorstellen staan beschreven.

Ontbreken van impact assessments

De Europese Commissie stelt dat Omnibussen alleen technisch van aard zijn en daardoor geen inbreuk op grondrechten maken. Dit zou betekenen dat er geen impact assessments van de voorgestelde veranderingen nodig zijn.⁴ Hier zijn ernstige twijfels over en er wordt gevreesd dat veel wijzigingen verder gaan dan de door de Commissie beoogde versimpeling.⁵ Staatssecretaris

¹ Raad van de Europese Unie 13 maart 2026, 7322/26, Proposal for a regulation of the European Parliament and of the Council amending Regulations (EU) 2024/1689 and (EU) 2018/1139 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI) – mandate for negotiations with the European Parliament, via:

<<https://data.consilium.europa.eu/doc/document/ST-7322-2026-INIT/en/pdf>> (geraadpleegd 21 april 2026).

² *Kamerstukken II* 2025/2026, 22 112, nr. 4287 (Kamerbrief van de staatssecretaris van Digitale Economie en Soevereiniteit aan de Tweede Kamer van 6 maart 2026, Naderend Raadscompromis Omnibus AI).

³ Europees Parlement 26 maart 2026, P10_TA(2026)0098, Simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI), via: <https://www.europarl.europa.eu/doceo/document/TA-10-2026-0098_EN.html> (geraadpleegd 21 april 2026).

⁴ Voorstel voor een verordening van het Europees Parlement en de Raad tot wijziging van Verordeningen (EU) 2024/1689 en (EU) 2018/1139 inzake de vereenvoudiging van de toepassing van geharmoniseerde regels inzake artificiële intelligentie (Digital Omnibus on AI), COM(2025) 836 final, p. 6; Voorstel voor een verordening van het Europees Parlement en de Raad tot wijziging van Verordeningen (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725 en (EU) 2023/2854 en Richtlijnen 2002/58/EC, (EU) 2022/2555 en (EU) 2022/2557 wat betreft de vereenvoudiging van het digitale wetgevingskader en tot intrekking van de Verordeningen (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868 en Richtlijn (EU) 2019/1024 (Digitale Omnibus), COM(2025) 837 final, p. 14-15.

⁵ *Kamerstukken II* 2025/26, 22 112, nr. 4302 (Brief van de tijdelijke commissie Grondrechten en Constitutionele toetsing inzake het EU-voorstel Digitale Omnibus AI, COM(2025) 836); *Kamerstukken II* 2025/26, 22 112, nr. 4301 (Brief van de tijdelijke commissie Grondrechten en Constitutionele toetsing inzake het EU-voorstel Digitale Omnibus Digitaal, COM(2025) 837); Equinet en European

Van Bruggen stuurt in dat kader een non-paper naar de Europese Commissie dat voorstelt alle wijzigingen aan de AVG in een aparte regelgevingsprocedure (met impact assessment) te behandelen.⁶

Omnibus AI

1. **Registratieplicht:** Het College maakt zich grote zorgen over het voorstel in de Omnibus AI om de registratieplicht te schrappen voor AI-systemen die geen hoog-risico zouden zijn, maar enkel ingezet worden voor beperkte of procedurele taken.⁷ Hierdoor is amper nog te controleren of deze classificatie rechtmatig is toegepast en zou dit door organisaties misbruikt kunnen worden om onder de verplichtingen van de AI-verordening uit te komen. Dit zou de uitvoerbaarheid van het toezicht ernstig beïnvloeden. Ook de Raad en het Europees Parlement lijken dit als problematisch te zien.
2. **Bevoegdheidsvermindering grondrechtenautoriteiten:** De AI-verordening verleent grondrechtenautoriteiten de bevoegdheid zelfstandig documentatie op te vragen van organisaties die hoog-risico AI-systemen gebruiken.⁸ Door de voorgestelde aanpassingen in de Omnibus AI zou deze bevoegdheid vervallen.⁹ Dit maakt het voor alle grondrechtenautoriteiten in de Europese Unie een stuk moeilijker om effectief toezicht op AI uit te voeren.
3. **AI-geletterdheid:** Hiernaast wordt door de Omnibus AI de verplichting voor alle AI-aanbieders en gebruiksverantwoordelijken om maatregelen te nemen die leiden tot een toereikend niveau van AI-geletterdheid bij hun personeel afgezwakt.¹⁰ AI-geletterdheid dient echter als noodzakelijke stap te worden gezien om in te kunnen schatten wanneer AI-inzet risico's voor grondrechten met zich brengt. Zowel de Raad als het Europees Parlement lijken dit voorstel wel enigszins te willen matigen.
4. **Biascorrectie:** Hoewel het doel van het voorstel om aanbieders meer mogelijkheden te bieden om data te testen op bias is aan te moedigen, is het zorgwekkend dat dit artikel de toegang tot bijzondere persoonsgegevens vergroot.¹¹ Hoewel de Raad en het Europees Parlement deze bevoegdheid weer enigszins willen inperken, blijft de Omnibus AI de AI-aanbieders op deze manier meer toegang geven tot bijzondere persoonsgegevens.

Network of National Human Rights Institutions (ENNHRI), Joint statement on the Digital Omnibus Regulation Proposals on AI and on Data, 12 maart 2026.

⁶ *Kamerstukken II 2025/2026*, 22112 nr. 4304 (Kamerbrief van de staatssecretaris van Justitie en Veiligheid aan de Tweede Kamer van 8 april 2026, Non-paper Digitale Omnibus – AVG)

⁷ Artikel 1(6) en 1(14) van de Omnibus AI

⁸ Artikel 77(1) van de AI-verordening

⁹ Artikel 1(26) van de Omnibus AI

¹⁰ Artikel 4 van de AI-verordening

¹¹ Art. 1(5) van de Omnibus Digitaal

Omnibus Digitaal

1. **Veranderen definitie persoonsgegevens:** De Omnibus Digitaal stelt voor om de vastgestelde AVG-definitie van een persoonsgegeven (art. 4(1) AVG) te wijzigen.¹² Hierbij wordt de classificatie van een persoonsgegeven afhankelijk van of de organisatie in kwestie de natuurlijk persoon over wie het gegeven gaat wel of niet kan identificeren, zelfs als een andere partij dat wel zou kunnen. Critici wijzen op de risico's voor fragmentatie, verminderde verantwoording, moeilijker toezicht en mogelijk gesjoemel met pseudonimisering van data, en daarmee op grote risico's voor het recht op gegevensbescherming en privacy.¹³
2. **Toegang tot persoonsgegevens als trainingsdata:** De Omnibus Digitaal maakt het mogelijk voor AI-ontwikkelaars om persoonsgegevens te gebruiken om AI-systemen te trainen, terwijl onder de huidige regelgeving hier vaak toestemming voor nodig is.¹⁴ De Omnibus Digitaal doet dit door voor te stellen dat het gebruiken van persoonsgegevens als trainingsdata altijd valt onder de AVG-grondslag van 'het gerechtvaardigd belang' van de ontwikkelaar, waardoor direct voldaan lijkt te zijn aan de AVG-eisen. Daarnaast maakt de Omnibus Digitaal het ook mogelijk om AI te trainen op bijzondere persoonsgegevens.¹⁵ Deze voorstellen vormen wederom een groot risico voor het recht op gegevensbescherming en privacy.¹⁶
3. **Geautomatiseerde besluitvorming:** Ook zorgt de Omnibus Digitaal ervoor dat het algemene verbod op geautomatiseerde besluitvorming vervalt. De Omnibus Digitaal vervangt namelijk het algemene verbod op geautomatiseerde besluitvorming uit art. 22 AVG met een lijst situaties waarin geautomatiseerde besluitvorming wel mogelijk is. Hierdoor wordt het voor individuen een stuk moeilijker om geautomatiseerde besluitvorming aan te vechten.¹⁷

¹² Artikel 3(1) van de Omnibus Digitaal

¹³ Zie voor een meer gedetailleerde uitleg hierover punt 3 van de European Data Protection Board (EDPB) en European Data Protection Supervisor (EDPS), Joint Opinion 2/2026 on the Proposal for a Regulation as regards the simplification of the digital legislative framework (Digital Omnibus), 11 februari 2026.

¹⁴ Artikel 3(15) van de Omnibus Digitaal dat een nieuw artikel 88c in de AVG voorstelt.

¹⁵ Art. 3(3) Omnibus Digitaal

¹⁶ Zie voor meer informatie hierover onderdeel 6 van de European Data Protection Board (EDPB) en European Data Protection Supervisor (EDPS), Joint Opinion 2/2026 on the Proposal for a Regulation as regards the simplification of the digital legislative framework (Digital Omnibus), 11 februari 2026

¹⁷ Zie voor meer informatie hierover onderdeel 7.3 van de European Data Protection Board (EDPB) en European Data Protection Supervisor (EDPS), Joint Opinion 2/2026 on the Proposal for a Regulation as regards the simplification of the digital legislative framework (Digital Omnibus), 11 februari 2026.

Position paper AP: Omnibus Digitaal en Omnibus AI

Vereenvoudiging van digitale regels is goed, zolang dit niet ten koste gaat van de bescherming van mensen. De Autoriteit Persoonsgegevens (AP) steunt het streven van de Europese Commissie met de zogenoemde Omnibus Digitaal en Omnibus AI: het stroomlijnen en verduidelijken van de huidige regels. Daar zijn bedrijven, toezichthouders én burgers bij gebaat.

Want dat het voor bedrijven lastig kan zijn om in het complexe landschap van regels producten en diensten te ontwikkelen die aan alle eisen voldoen, dat snapt de AP. Het is positief dat daar aandacht voor is en dat er concrete voorstellen worden gedaan om (digitale) wetgeving te verhelderen en regeldruk te verminderen.

De regels geven vorm aan een grondrecht dat wij burgers allemaal hebben en dat ons beschermt in een digitale wereld die snel verandert. De AP benadrukt: innovatie en bescherming kunnen en moeten hand in hand. Zorgen we daar niet voor, dan brengt dat grote risico's met zich mee.

De omnibussen treffen deze balans niet goed. De voorstellen hierin gaan soms veel verder en stellen ingrijpende of onduidelijke wijzigingen voor van de Algemene verordening gegevensbescherming (AVG) en de AI-verordening, zonder een goede afweging van de gevolgen voor de bescherming van burgers.

Dit betekent dat hoewel sommige voorgestelde wijzigingen organisaties en mensen potentieel kunnen helpen, andere wijzigingen diep ingrijpen in grondrechten. **De AP denkt graag mee over vereenvoudiging, maar de kern van de bescherming van de rechten van mensen moet intact blijven en mensen moeten op digitale regels kunnen blijven vertrouwen.** Te gehaaste besluitvorming over de omnibusvoorstellen kan ten koste gaan van de bescherming van burgers én de rechtszekerheid voor bedrijven en organisaties.

Zo signaleert de AP onder andere:

- *Ingrijpende wijziging van de definitie persoonsgegevens in de AVG: houd de definitie zoals die is, zodat het helder blijft wat wel en niet een persoonsgegeven is. Onduidelijkheid daarover verzwakt bescherming én toezicht.*
- *Minder transparantie en verantwoording betekent minder effectief toezicht: deze waarborgen moeten we niet schrappen.*
- *Minder bewustwording over AI: organisaties moeten zelf verantwoordelijk blijven voor de kennis en vaardigheden over AI van hun mensen.*
- *Minder duidelijkheid: veel van de voorstellen zijn zo onduidelijk geformuleerd dat ze de problemen niet oplossen.*

De AP ziet daarnaast ook positieve voorstellen die meer duidelijkheid bieden door het toezicht te versterken en definities op Europees niveau te uniformeren.

Onze zorgen en adviezen lichten we hieronder verder toe.

1. Ingrijpende wijziging van de definitie persoonsgegevens in de AVG: houd de definitie zoals die is, zodat het helder blijft wat wel en niet een persoonsgegeven is. Onduidelijkheid daarover verzwakt bescherming én toezicht.

Hoewel sommige aanpassingen uit de omnibusvoorstellen technisch lijken, kunnen ze grote gevolgen hebben in de praktijk. De wet moet helder blijven over bijvoorbeeld wat wel en niet een persoonsgegeven is. De Omnibus Digitaal verandert belangrijke basisbegrippen zoals 'persoonsgegevens' en 'pseudonimisering'. Deze definities vormen de kern van het grondrecht op bescherming van persoonsgegevens: welke gegevens wel én niet meer worden beschermd.

De Commissie verwijst daarbij naar een recente uitspraak van het Hof van Justitie van de EU, maar de wijzigingen gaan verder dan die uitspraak. Bovendien trekt de Commissie toekomstige verdere uitleg van die definities naar zich toe. Daardoor kan het voor organisaties en burgers onduidelijk worden welke gegevens nu precies persoonsgegevens zijn en welke niet. Ook zorgt dit ervoor dat de bescherming van sommige (gepseudonimiseerde) persoonsgegevens in het geding komt. Mensen zijn dus minder goed beschermd en toezichthouders hebben minder zicht op risico's.

De AP benadrukt dat alle gegevens aan de hand waarvan burgers kunnen worden gevolgd en geprofileerd persoonsgegevens zijn en binnen de bescherming van het grondrecht moeten blijven vallen. Alleen zo houden burgers grip op hun (digitale) identiteit.

2. Minder transparantie en verantwoording betekent minder effectief toezicht: deze waarborgen moeten we niet schrappen.

Een digitale samenleving kan zich alleen verder ontwikkelen als burgers erop kunnen vertrouwen dat dit op een betrouwbare en veilige manier gebeurt. Dan moet iedereen zijn rol kunnen vervullen. Toezichthouders moeten zicht kunnen houden op risico's zodat wij op tijd kunnen ingrijpen en bijsturen. Organisaties zelf moeten zorgen voor verantwoording en transparantie. Burgers moeten grip houden op hun gegevens. Bij sommige voorstellen zien we het risico dat dit moeilijker wordt.

Zo gaat volgens de huidige voorstellen de drempel omhoog voor het melden van datalekken bij de toezichthouder op grond van de AVG: organisaties moeten dan alleen nog melden als zij een hoog risico zien voor burgers. In de praktijk zien we echter dat organisaties de risico's van een datalek vaak (bewust of onbewust) onderschatten.¹ Dit gebeurde vorig jaar: bij een bedrijf waren de contactgegevens (naam, adres en e-mailadres) en financiële gegevens van 1,5 miljoen klanten gelekt. Het bedrijf had het risico te laag ingeschat en daarom waren niet alle klanten hierover geïnformeerd. De AP heeft ervoor gezorgd dat alle getroffen mensen alsnog op de hoogte werden gesteld, zodat zij op hun hoede konden zijn voor nepberichten en oplichting. Met deze wijziging uit de omnibusvoorstellen heeft de AP geen zicht meer op deze gevallen: zo gaat de 'corrigerende' functie van de meldplicht verloren en verliezen mensen de controle over hun gegevens. De AP vindt dat de drempel moet blijven zoals die is. Wel ziet de AP het als haar rol om te kijken hoe de AP het melden zo makkelijk kan maken voor organisaties.

Bepaalde AI-systemen met hoge risico's zijn uitgezonderd van de specifieke (product)eisen voor deze categorie systemen, als deze geen significant risico vormen voor gezondheid, veiligheid of grondrechten. Bijvoorbeeld omdat het systeem enkel een beperkte procedurele stap uitvoert. Voor deze AI-systemen bestaat wel een

¹ Zo onderschatte in 2023 gemiddeld 69% van de organisaties die getroffen werden door een ernstige cyberaanval het risico voor de getroffen personen. In 54% van de gevallen (in totaal 330 datalekken) werden de getroffen personen na een ernstige cyberaanval niet geïnformeerd, terwijl dit wel had gemoeten.

publieke registratieplicht, zodat duidelijk is dat de aanbieder gebruik heeft gemaakt van deze uitzonderingsgrond en het AI-systeem daarom geen CE-keurmerk bevat. Deze verplichting wordt in de Omnibus AI afgeschaft. Potentieel risicovolle systemen vallen hierdoor buiten het zicht van het publiek en de toezichthouder, waardoor het risico op gevaarlijke incidenten toeneemt.

3. Minder bewustwording over AI: organisaties moeten zelf verantwoordelijk blijven voor de kennis en vaardigheden over AI van hun mensen.

Om verantwoord en veilig nieuwe technologieën zoals AI in te zetten en verder te ontwikkelen, is het essentieel dat organisaties eerst begrijpen wat AI is en hoe ze ermee om moeten gaan. Organisaties die AI inzetten of zelf ontwikkelen moeten ook verantwoordelijk zijn voor het opleiden van hun personeel zodat dat zelf in staat is risico's (en kansen) van AI te herkennen en snel op te treden. De Omnibus AI verlegt deze verantwoordelijkheid van organisaties zelf naar de overheid.

De algemene verplichting voor ontwikkelaars en gebruiksverantwoordelijken van AI om te zorgen voor AI-geletterdheid wordt namelijk afgeschaft. In plaats daarvan worden de Commissie en de lidstaten verplicht om maatregelen te nemen om AI-geletterdheid te stimuleren. Dit is wat betreft de AP ongewenst en onpraktisch. AI-geletterdheid bestaat uit vaardigheden, kennis en begrip over AI en is een kernvoorwaarde voor verantwoorde ontwikkeling en gebruik van AI. Organisaties kunnen juist zelf het beste beoordelen wat er specifiek nodig is binnen hun organisatie. De AP is daarom van mening dat de verplichting moet blijven, maar wel met de nadruk op een risicogebaseerde aanpak. De Commissie en lidstaten kunnen organisaties wel ondersteunen op dit gebied, zoals de AP ook al eerder heeft gedaan.²

4. Minder duidelijkheid: veel van de voorstellen zijn zo onduidelijk geformuleerd dat ze de problemen niet oplossen.

Er zijn meerdere wijzigingen die nieuwe vragen oproepen. Dit kan leiden tot rechtsonzekerheid en daarmee juist meer regeldruk bij organisaties en de toezichthouder, en de ondermijning van de huidige bescherming. Oftewel: met deze formulering worden problemen bij organisaties dus helemaal niet opgelost.

Zo wordt voorgesteld om in de AVG het recht op inzage te beperken als er sprake is van buitensporige verzoeken. Alleen zijn de criteria voor wat geldt als een buitensporig verzoek heel breed geformuleerd. Dit kan betekenen dat burgers minder goed inzage krijgen in hun gegevens én dat mogelijk nieuwe administratieve last ontstaat. Organisaties zullen nieuw beleid moeten maken om te beoordelen wat 'buitensporig' is en dit mogelijk verschillend uitleggen.

Voor de AI-verordening stelt de Commissie voor om de implementatie van de regels voor AI met hoge risico's uit te stellen. Richting aanbieders en gebruiksverantwoordelijken vermindert dit de urgentie om beschermende maatregelen te nemen. Dit voorstel zorgt ook voor veel onzekerheid: als het niet lukt om de omnibus vóór 2 augustus 2026 in werking te laten treden, zullen de vereisten voor AI met hoge risico's vanaf dat moment van toepassing zijn om vervolgens eventueel tijdelijk weer gepauzeerd te worden.

De Commissie wil ten slotte graag duidelijkheid scheppen over het gebruik van gegevens voor AI-systemen. Zo stelt de Omnibus Digitaal voor om expliciet in de AVG op te nemen dat gerechtvaardigd belang gebruikt kan worden als een grondslag voor het gebruik van persoonsgegevens voor de ontwikkeling en werking van AI-

² Zie de AP-website: [AI-geletterdheid](#).

systemen. Alleen creëert dit mogelijk juist minder duidelijkheid. Op het moment wordt deze grondslag niet uitgesloten, maar de aanbieders of ontwikkelaars moeten altijd nagaan of het de meest geschikte grondslag is en een belangenafweging maken.³ Deze bepaling suggereert een verruiming die er niet is. In andere woorden: deze wijziging is overbodig en creëert alleen meer verwarring.

5. Positieve voorstellen: de AP verwelkomt voorstellen die meer duidelijkheid bieden door het toezicht te versterken en definities op Europees niveau te uniformeren.

Natuurlijk zijn er ook voorstellen in de Omnibussen die de huidige regels duidelijker maken voor burgers én organisaties en het toezicht versterken. Hier zijn wij erg blij mee en we staan klaar om de wetgever bij te staan om deze wijzigingen zo goed en helder mogelijk vast te leggen en daarna in de praktijk te brengen.

We denken daarbij aan de aanpassingen die ten voordeel komen van organisaties en bedrijven. Een voorbeeld is het voorstel voor templates op Europees niveau, zodat organisaties en bedrijven zich makkelijker kunnen houden aan de regels, ook als ze in meerdere Europese landen actief zijn. Dit zijn o.a. templates voor het uitvoeren van een DPIA (Data Protection Impact Assessment), en het melden van datalekken en van lijsten met concrete voorbeelden van activiteiten waarvoor je een DPIA moet opstellen ('black list'), maar ook wanneer dit niet nodig is ('white list'). Het opstellen van dergelijke templates moet dan wel een zaak van de toezichthouders blijven.

Daarnaast overweegt de Commissie om de regels en het toezicht rondom functionele en analytische cookies op Europees niveau te harmoniseren, en om regels te maken over wanneer je opnieuw om toestemming kan worden gevraagd en je toestemming automatisch in je browser laten opslaan. De AP vindt dat een heel goed streven. Dit kan keuzemoeheid bij burgers verminderen, waardoor zij beter geïnformeerde en beter doordachte keuzes kunnen maken. Wel zijn er helaas ook bij dit voorstel nog vragen en zorgen die beantwoord moeten worden.

Ten slotte is er in de Omnibus AI ook aandacht voor het versterken van samenwerking tussen toezichthouders. Dat moedigt de AP aan: de AP staat als coördinerende toezichthouder op AI en algoritmes en als grondrechtentoezichthouder voor een sterke, loyale samenwerking tussen toezichthouders.⁴ De AP geeft hier op het gebied van de AI-verordening samen met de Rijksinspectie Digitale Infrastructuur (RDI) al vorm aan.

De AP roept de wetgever op om kritisch te kijken naar de voorgestelde wijzigingen in de omnibusvoorstellen. De AP ziet dat veel van deze zorgen al worden gedeeld door het kabinet in de appreciatie. Als concrete vervolgstap zal de AP op grond van haar AVG-taak samen met de andere Europese privacytoezichthouders een uitgebreide, gezamenlijke analyse geven. Daarin zal de AP ook ingaan op de voorstellen die hier niet aan bod zijn gekomen.

³ Zie ook de EDPB-opinie over AI-modellen van december 2024: [EDPB opinion on AI models: GDPR principles support responsible AI](#).

⁴ Het is essentieel voor de effectiviteit van het toezicht dat de bepalingen in de Omnibus AI over loyale samenwerking tussen toezichthouders worden vormgegeven op een manier zodat deze samenwerking soepel kan verlopen zonder barrières die deze effectiviteit ondermijnen.

De Digitale Omnibus zwakt fundamentele Europese rechten af

23 April 2026

In de Digitale Omnibus en de Digitale Omnibus AI doet de Europese Commissie afbreuk aan onze fundamentele mensenrechten. Onder het mom van 'simplificatie' en het 'stimuleren van innovatie' worden de poten onder het gegevensbeschermingsrecht weggezaagd. De voorstellen hebben bovendien weinig met het versimpelen of het verminderen van administratieve lasten van doen.

Hier wordt ook voor gewaarschuwd in het Fiche Omnibus AI en Omnibus Digitaal van de minister van Buitenlandse Zaken.¹ We onderschrijven de risico's die in het fiche naar voren worden gebracht en zien graag dat daar ook gevolg aan wordt gegeven. Daarom brengen we de belangrijkste voorgestelde wijzigingen in digitale wetgeving onder uw aandacht. Bits of Freedom en Stichting Data Bescherming Nederland adviseren de voorstellen die gedaan worden in de Digitale Omnibussen af te wijzen en vast te houden aan de fundamentele waarden die Europa eigen zijn, juist nu deze waarden in geopolitieke verhoudingen onder druk komen te staan.

De vernauwing van het begrip persoonsgegevens

De Europese Commissie stelt voor om de definitie van persoonsgegevens aan te passen. Onder de huidige definitie is alle data dat tot een persoon te herleiden is een persoonsgegeven. Dus niet alleen data dat een individu direct identificeert, maar ook data dat indirect naar een individu te herleiden is (zoals gepseudonimiseerde data) valt onder de AVG. Alleen volledig geanonimiseerde data valt niet onder de definitie van persoonsgegevens. De drempel voor daadwerkelijke anonimisering ligt echter hoog, omdat het doorgaans slechts een beperkt aantal datapunten vereist om een individu te her-identificeren.

In de Digitale Omnibus stelt de Europese Commissie voor dat gepseudonimiseerde persoonsgegevens in de toekomst echter enkel een persoonsgegeven zijn als de data controller waarschijnlijk over de middelen beschikt om die te herleiden tot een persoon. Dus, wat voor één organisatie een persoonsgegeven is, is dat voor de ander niet. Dit druist in tegen het huidige beschermingsniveau, creëert juist méér juridische onzekerheid en compliceert de handhaving van de AVG.

1

https://www.tweedekamer.nl/debat_en_vergadering/commissievergaderingen/details?id=2025A08254

De definitie van persoonsgegevens vormt de basis van zowel de AVG als andere digitale regelgeving. Een dusdanige verandering heeft dan ook vergaande gevolgen en kan niet als vereenvoudiging worden gezien. We zijn dan ook blij om te zien dat de Nederlandse overheid in haar fiche eenzelfde standpunt heeft ingenomen en moedigen de overheid aan deze koers vast te houden. We zien bovendien graag dat de Nederlandse overheid recital 27a (in de laatste draft van de Europese Raad) verwijderd.

Verzwakking van het verbod op het verwerken van bijzondere persoonsgegevens in AI systemen

Op grond van de AVG is de verwerking van bijzondere persoonsgegevens in beginsel verboden. En dat is niet voor niets. Gegevens over iemands gezondheid, seksualiteit, etniciteit, politieke of religieuze opvatting zeggen veel over een persoon en kunnen gebruikt worden om individuen en groepen te discrimineren, onder druk te zetten, of op een andere manier te benadelen.

In Nederland zien we een reeks aan voorbeelden waaruit blijkt dat algoritmen discrimineren op grond van gender, etniciteit of religie.² Discriminatie neemt bovendien regelmatig een indirecte vorm aan: niet via expliciete categorieën als nationaliteit, gender of religie, maar via schijnbaar neutrale criteria die in de praktijk dezelfde groepen treffen. Dit is een welbekend probleem en wordt al jaren aangehaald als een belangrijk risico bij het gebruik van algoritmen en AI.

Ondanks deze enorme risico's wil de Europese Commissie het makkelijker maken om bijzondere persoonsgegevens te verwerken. Namelijk, als het voor een data controller te omslachtig is om deze bijzondere persoonsgegevens uit een dataset te halen, kunnen deze alsnog worden gebruikt om AI-modellen te trainen. Daarmee wordt het verbod op de verwerking van persoonsgegevens verzwakt, daar waar dit verbod juist essentieel is. De vraag of het verwijderen van bijzondere persoonsgegevens omslachtig is, is bovendien geheel subjectief. Zeker bij het gebruik van ongestructureerde datasets zou een bedrijf te makkelijk bij voorbaat al kunnen stellen dat het te kostbaar is om deze gegevens te verwijderen.

Hiermee opent de Europese Commissie de deur naar de grootschaligere verwerking van bijzondere persoonsgegevens, en ondermijnt zij het verbod op discriminatie, ons recht op privacy, vrijheid van meningsuiting en godsdienstvrijheid. Daarmee wordt het nog eenvoudiger om te discrimineren met AI, bedoeld of onbedoeld. Bovendien kunnen gegevens over iemands seksuele voorkeur, gedrag en zelfs iemands biometrische

2

<https://www.volkskrant.nl/columns-opinie/opinie-zolang-de-overheid-een-onstilbare-datahonger-heeft-heb-ben-kinderen-alle-reden-zich-onveilig-te-voelen~bb173fd6/>

gegevens op grote schaal verwerkt worden. Dit druist volledig in tegen de meest fundamentele rechten, waaronder het verbod op discriminatie, de vrijheid van meningsuiting, het recht op privacy en godsdienstvrijheid.

Legitimeren van het gebruik van persoonlijke data om AI te trainen

De datahonger van AI bedrijven staat op gespannen voet met twee beginselen van de AVG: dataminimalisatie en doelbinding. Samen zorgen deze beginselen ervoor dat individuen niet worden blootgesteld aan onnodige risico's en dat gegevens niet blijven rondzwerven op een manier die op een later moment schade kan veroorzaken.

Het datalek bij Bevolkingsonderzoek Nederland illustreert treffend wat er fout kan gaan als we deze beginselen vergeten: het laboratorium beschikte over veel meer data dan strikt noodzakelijk, waaronder de BSN nummers van meer dan 700.000 Nederlanders. Die data ligt nu op straat.

Met de toevoeging van Artikel 88c aan de AVG lijkt de Europese Commissie de datahonger van Big Tech bedrijven echter te willen legitimeren. Het rechtmatig gebruik van persoonsgegevens voor het trainen van AI vereist ofwel de toestemming van de betrokkene, of een andere rechtmatige grondslag. Artikel 88c biedt verwerkingsverantwoordelijken een nieuwe rechtmatige grondslag voor het gebruik van persoonsgegevens: de ontwikkeling en het gebruik van AI-systemen. In feite wordt de technologie hier zelf het doel, en daarmee wordt gebroken met de technologie neutraliteit van de AVG.

En hoewel artikel 88c vereist dat betrokkenen de mogelijkheid hebben om zich af te melden voor het gebruik van hun persoonsgegevens, zullen zij daar in de praktijk moeite mee hebben. Gebruikers weten vaak niet dat hun gegevens überhaupt worden gebruikt. Bovendien, zodra de gegevens zijn gebruikt om een model te trainen, is de enige manier om dat terug te draaien het model opnieuw te trainen, met een nieuwe dataset waarin de persoonsgegevens niet voorkomen.

Een studie in opdracht van NOYB, uitgevoerd door Gallup, stelt dat slechts 7% van de Duitsers zou willen dat Meta hun persoonsgegevens, waaronder Instagram-berichten en foto's, gebruikt om zijn AI te trainen.³ Dit suggereert dat, hoewel Big Tech dit gebruik misschien als legitiem beschouwt, gebruikers het daar niet mee eens zijn.

³

<https://noyb.eu/en/noyb-survey-only-7-users-want-meta-use-their-personal-data-ai>

Automatische beslissingen door algoritmes worden genormaliseerd

De wijziging van Artikel 22 AVG in het Digital Omnibus zal het voor organisaties makkelijker maken om AI-systemen te gebruiken voor het nemen van geautomatiseerde beslissingen, zoals het besluit om iemand een lening of hypotheek te verstrekken. Dit voorstel negeert jaren aan onderzoek naar de negatieve impact van automatische beslissingen op burgers en consumenten.

Ter illustratie: de Autoriteit Persoonsgegevens heeft recent vastgesteld dat het gebruik van geautomatiseerde scanauto's door politie heeft geleid tot ongeveer een half miljoen onterechte parkeerboetes per jaar. Scanauto's genereren automatisch beelden van mogelijke parkeerovertredingen, die vervolgens worden beoordeeld door menselijke controleurs. Zonder de juiste context zijn controleurs echter vaak niet in staat om correct te beoordelen of er een overtreding heeft plaatsgevonden, wat resulteert in een foutpercentage van 10%.

Dit voorbeeld onderstreept een breder probleem met de manier waarop automatische beslissingen vooroordelen en schade opschalen. Omdat geautomatiseerde systemen grote aantallen gevallen tegelijkertijd verwerken, kan zelfs een klein foutpercentage op grote schaal veel schade teweegbrengen. Deze parkeerzaak benadrukt verder dat de aanwezigheid van een zogeheten 'human in the loop' deze problemen niet noodzakelijkerwijs vermindert. Onderzoek naar 'automatisering bias' suggereert dat mensen vaak de voorkeur geven aan het oordeel van een machine, in plaats van een onafhankelijk oordeel te vormen, met name wanneer zij niet beschikken over de contextuele informatie die nodig is om een zaak op zijn merites te beoordelen⁴. Dit effect kan worden versterkt door wat 'selectieve naleving' genoemd wordt: de neiging van mensen om algoritmische aanbevelingen te volgen wanneer deze overeenkomen met reeds bestaande stereotypen, en de aanbevelingen te negeren wanneer dat niet het geval is.

Gelet op het bovenstaande zijn wij van mening dat automatische beslissingen zeer beperkt moeten worden ingezet en dat de wijzigingen van Artikel 22 AVG moeten worden verworpen.

Het verzwakken van de AI-Verordening

De AI-Verordening is in 2024 aangenomen, als resultaat van jarenlange onderhandelingen en brede democratische besluitvorming. Echter, nog voordat de verordening volledig in werking is getreden, worden de overeengekomen waarborgen én

⁴ <https://academic.oup.com/jpart/article/33/1/153/6524536>

het democratische proces ondermijnd. De Europese Commissie wil nu al belangrijke rechten en plichten afbreken, en de implementatietermijn uitstellen. Zo wordt voorgesteld om de registratieplicht voor hoog-risico AI-systemen af te schaffen, als de aanbieder zelf geen belangrijk risico ziet voor de gezondheid, veiligheid of grondrechten. Daarmee wordt er heel veel ruimte en vrijheid aan aanbieders gegeven en wordt de transparantie van, en de controle op AI-toepassingen beperkt. Ook wil de Europese Commissie uitstellen dat verkopers van gevaarlijke AI-toepassingen beboet kunnen worden. Het geeft verkopers van dit soort toepassingen dus de vrije hand, ten koste van de mensen die door dit soort toepassingen geraakt worden.

Fundamentele rechten in woord én daad beschermen

De Europese Commissie stelt een “makkelijker en sneller” Europa te willen om innovatief en competitief te zijn. Daarbij belooft de Europese Commissie om fundamentele rechten niet af te zwakken. Echter, vervolgens komt de Europese Commissie met voorstellen die weinig met vereenvoudiging of het verlichten van administratieve lasten te maken hebben en die wel degelijk belangrijke beschermingen van fundamentele rechten afbreken.

Bovendien zorgt de afzwakking van rechten en het rommelen aan wettelijke verplichtingen ervoor dat er onduidelijkheid ontstaat over het doel van de wetgeving en over de naleving daarvan. Als bijzondere persoonsgegevens te privacygevoelig zijn om te verwerken, waarom mogen ze dan wel op grote schaal verwerkt worden om AI systemen te trainen, terwijl de risico's juist bij die technologie bekend zijn? Als het steeds makkelijker wordt om personen te identificeren door het koppelen van informatie uit verschillende databronnen, waarom zouden sommige gepseudonimiseerde gegevens straks dan niet meer onder de AVG vallen? En waarom wordt er van een nieuwe AI wet een papieren tijger gemaakt, door de handhaving uit te stellen? Deze afzwakkingen van Europese wetgeving zijn niet in het belang van burgers en dragen weinig tot niets bij aan het verlichten van administratieve lasten.

Een groot deel van de Europese bedrijven zit hier ook niet op te wachten. Uit onderzoek van de Europese Commissie naar de AVG blijkt dat maar liefst 96% van de respondenten aangeeft dat de voordelen van privacy-investeringen zwaarder wegen dan de kosten. Een sterke privacy cultuur versterkt de reputatie van bedrijven en wekt vertrouwen bij hun klanten. Ook geeft een grote meerderheid van de bedrijven aan dat zij de AVG een gebalanceerd juridisch raamwerk vinden.⁵ De noodzaak tot grote wijzigingen in de AVG wordt dan ook onvoldoende onderbouwd.

⁵

<https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-regulation-proposal> / Staff working document pagina 34 e.v.

Als de wijzigingsvoorstellen niet ten voordele van Europese burgers en bedrijven zijn, wie profiteert er dan van het afzwakken van Europese rechten? Uit een analyse van Corporate Europe Observatory en LobbyControl blijkt dat veel belangrijke wijzigingen die in de Digitale Omnibussen staan overeenkomen met de lobby posities van Big Tech bedrijven.⁶ Maar Europees recht, waaronder de AI-verordening en het gegevensbeschermingsrecht zijn bedoeld om burgers te beschermen, niet om Big Tech bedrijven nog rijker te maken ten koste van mensenrechten. Dit is dan ook hét moment voor Nederland en de Europese Unie om vast te houden aan fundamentele rechten en waarden en te beschermen wat belangrijk is.

De voorstellen van de Europese Commissie komen niet overeen met het doel dat de Europese Commissie stelt te hebben. Ook wordt de belofte om fundamentele rechten te waarborgen gebroken. Dit wordt ook opgemerkt in het fiche. Wij roepen de Nederlandse overheid dan ook op haar koers vast te houden, in woord en daad. De Nederlandse overheid dient zich uit te spreken voor het belang van Nederlandse en Europese burgers en (midden en klein) bedrijven en daarom de voorgestelde wijzigingen af te wijzen.

Met vriendelijke groet,

Nadia Benaissa
namens Bits of Freedom

Anouk Ruhaak
namens Stichting Data Bescherming Nederland

6

<https://corporateeurope.org/en/2026/01/article-article-how-big-tech-shaped-eus-roll-back-digital-rights>

DIGITAL OMNIBUS

Positie Paper VNO-NCW and MKB-Nederland ten behoeve van Eerste Kamer

11 mei 2026

Digital Omnibus– positie VNO-NCW en MKB-Nederland

VNO-NCW en MKB-Nederland verwelkomen dat de Europese Commissie het omvangrijke en complexe Europese digitale en dataregelgevingskader beter geharmoniseerd, voorspelbaar, proportioneel, coherent en uitvoerbaar wil maken. Dat vermindert onnodige lasten voor bedrijven en bevordert verantwoorde innovatie en toepassing van AI, andere technologieën en data, zonder afbreuk te doen aan de doelstellingen van de Europese digitale regelgeving.

Het voorstel van de Europese Commissie vormt door de bank genomen een goede *eerste* (herstel)stap. Er zijn echter ook zorgen over onderdelen van het Digital Omnibus voorstel.

Het mag niet bij deze omnibus blijven, er zijn meerdere stappen nodig om echt het verschil te maken.

Digital Omnibus

Gerichte aanpassingen AVG

VNO-NCW en MKB-Nederland steunen de voorgestelde gerichte aanpassingen van de AVG. Bedrijven hebben last van de verschillen in de uitleg van de AVG tussen de toezichthouders in de EU. Het voorstel van de Europese Commissie vormt een democratisch antwoord op de vele signalen dat de AVG tekortschiet waar het gaat om risico proportionaliteit.

Volgens het Draghi-rapport over concurrentievermogen uit 2024 kunnen de nalevingskosten van de AVG oplopen tot EUR 500.000 voor het mkb en EUR 10 miljoen voor grotere organisaties.

Het is goed dat het voorstel interpretatieverschillen probeert tegen te gaan. Bijvoorbeeld wat betreft de definitie van persoonsgegevens, de definitie van wetenschappelijk onderzoek en gerechtvaardigd belang als verwerkingsgrondslag. Het voorstel bevat daarmee geen grote wijzigingen.

Ook probeert de Europese Commissie breder meer duidelijkheid te scheppen. Denk aan een geharmoniseerd DPIA format en dat toezichthouders duidelijker aangeven wanneer wel/niet een DPIA vereist is.

Verder doet de Europese Commissie concrete voorstellen om de uitvoering van de AVG meer proportioneel en risicogericht te maken. Door het melden van hoog-risico datalekken, het tegengaan van misbruik of excessief gebruik van het recht op inzage en dat er geen privacy statement nodig is als informatie bekend verondersteld mag worden.

Ontbrekende elementen AVG

De voorstellen zijn echter (nog) niet allemaal perfect en er ontbreken enkele belangrijke elementen. Zo ontbreekt een uitzondering voor het verwerken van residu strafrechtelijke gegevens. Ook gaat het voorstel geheel voorbij aan het verschil tussen het verwerken van bijzondere persoonsgegevens van reguliere personen en van publieke personen. Denk bijvoorbeeld aan de geloofsovertuiging van religieuze leiders en strafrechtelijke feiten gepleegd door (buitenlandse of binnenlandse) overheidspersonen. Het recht op informatie (artikel 11 Handvest) dient bij publieke personen afgewogen te worden tegen het recht op bescherming van persoonsgegevens.

Cookies, ePrivacy en toestemming

VNO-NCW en MKB-Nederland zouden graag zien dat de samenloop tussen de ePrivacy-richtlijn en de AVG wordt vereenvoudigd. De huidige samenloop leidt tot juridische onzekerheid, hogere nalevingskosten en versnipperd toezicht. Het voorstel van de Europese Commissie bevat ter zake de samenloop van de AVG en de ePrivacy richtlijn echter (nog) geen verbetering.

Single Entry Point voor incidentmeldingen

VNO-NCW en MKB-Nederland zijn geen voorstander van één centraal Europees platform.

Een dergelijk centraal platform kan een aantrekkelijk doelwit worden voor criminelen en statelijke actoren en daarmee risico's voor cyberveiligheid en nationale veiligheid vergroten.

De voorkeur gaat uit naar één nationale meldpagina per lidstaat voor meldingen voor onder meer NIS2, CER, CRA en AVG met doorgeleiding naar de relevante toezichthouders en – waar vereist - doorgeleiding via de nationale geharmoniseerde meldpagina's van de andere lidstaten naar toezichthouders in de andere lidstaten. In Luxemburg hebben ze een meldpagina voor de verschillende incident meldingen ingericht, dit kan als voorbeeld dienen voor de andere meldpagina's in de EU.

Data Act en datadeling

VNO-NCW en MKB-Nederland steunen de consolidatie van de Data Governance verordening (DGA), de Open Data richtlijn en de Vrij-verkeer van niet persoonsgebonden data richtlijn in de Data Act, dit verbetert de coherentie en rechtszekerheid. Wel is nog duidelijkheid nodig over het samenspel tussen de Data verordening en de AVG.

Naast dat we positief zijn over de consolidatie zijn we ter zake de voorgestelde aanpassingen van de Data Act ook positief over de voorstellen voor:

- Data-intermediairs: de huidige verplichting tot juridische scheiding van diensten is economisch belemmerend; het voorstel voor een functionele scheiding en vermindering van de verplichtingen is beter uitvoerbaar.
- Voorkomen van lekken bedrijfsgeheimen naar derde landen waar onvoldoende bescherming is. Er moet echter worden voorkomen dat individuele ondernemingen, vooral mkb-bedrijven, kostbare analyses van buitenlands recht moeten uitvoeren. De Commissie en lidstaten zouden algemene ondersteuning moeten bieden.
- Het beperken van B2G-datadeling tot publieke noodsituaties; en
- Een lichter cloud-switch regime voor maatwerkclouddiensten die vóór 12 september 2025 zijn overeengekomen (mits het begrip maatwerk niet te ruim wordt uitgelegd).

Irvette Tempelman
VNO-NCW/MKB-Nederland
5.1.2.e @vnoncw-mkb.nl

DIGITAL OMNIBUS AND OMNIBUS ON AI

Position Paper VNO-NCW and MKB-Nederland

9 February 2026

VNO-NCW and MKB-Nederland welcome the simplification efforts of the European Commission to make the vast and complex digital & data rules more harmonized, predictable, proportionate, coherent and easier to implement. This reduces the burden on companies, increases responsible (innovative) development and adoption of AI without lowering the objectives of the Rulebook.

The Digital omnibus and the Omnibus on AI presented by the European Commission on 19th November, are a good first step towards this and we hope more will follow¹. Although we support many of the efforts, we also have some concerns, specifically regarding the proposal for a Single entry Point for cyber- and privacy incidents.

Summary

Omnibus on AI

We support the proposals set out in the Omnibus on AI where they strengthen legal certainty and make compliance more workable. This includes the proposal to postpone deadlines for high-risk AI obligations to allow time for the development of standards and clearer guidance on the AI Act and its interaction with other EU rules. However, we are concerned about the possibility for the Commission to decide on an earlier deadline once the standards and guidance are published. We would prefer a fixed and realistic deadline to avoid legal uncertainty about the date of application, focus on high quality clarification and ensure that notified bodies² can be formally notified on time to perform the

¹ We refer to the position papers of BusinessEurope with many examples of inconsistencies, unclarities and overlaps¹ which need addressing: [Reducing regulatory burden to restore the EU's competitive edge - BusinessEurope](#) (December 2025); [Simplifying the EU digital rulebook - a BusinessEurope position paper - BusinessEurope](#) (July 2025)

² With regard to annex I high risk AI systems

required third party conformity assessments.³

We also support the proposal allowing (under strict safeguards) exceptional processing of special categories of personal data for bias detection & mitigation to prevent discrimination beyond high-risk AI. In addition, we back the proposals to oblige the Commission and Member States to promote AI literacy and skills (not limited to the working force), to remove disproportionate EU database registration for low-risk AI systems that fall within the broad scope of Annex III but are not high-risk applications, to extend simplified quality management system approaches from micro-enterprises to SMEs and improving cooperation among competent authorities. We also support the extension of real-world testing to high-risk AI systems embedded in products.

Digital Omnibus

We also support key proposals in the Digital Omnibus aimed at clarifying and better aligning GDPR with the wider digital framework. This includes proposals for targeted GDPR amendments to improve consistency, to clarify the demarcation between pseudonymised and personal data, and to explicitly confirm that “scientific research” covers academic, industrial and SME R&D, subject to the strict safeguards in the GDPR⁴. We support proposals to address the handling of special-category data in AI datasets, including clarification that residual traces may remain where removal is disproportionate after appropriate preventive measures have been taken, coupled with an obligation to apply effective measures to prevent disclosure or reappearance in outputs. We also support the proposal to confirm that legitimate interest can serve as a legal basis for developing and operating AI, subject to the usual balancing test and full compliance with GDPR principles and obligations. However, for legal certainty and level playing field purposes, we call for improving the clarity of aforementioned proposals.

Also, we welcome the Digital Omnibus proposals for burden reduction: including a more proportionate approach of access rights (in the event of misuse of rights), exception to information duties where individuals already have the information, and more proportionate breach notification requirements (e.g., notifying authorities only of high-risk breaches, using a harmonised template, and applying a more realistic 96-hour deadline). However, we call for improving the clarity of the proposals to ensure legal certainty. In the context of burden reduction, we also support the proposals for harmonised DPIA lists, templates and methodologies; further consolidation of data rules in the Data Act; and – for the enablement of data spaces - a more proportionate regime for data intermediation services through functional (rather than legal) separation and reduced obligations. In addition, we support stronger trade secret protections to

³ Such notification process takes around a year.

⁴ Article 89 GDPR

refuse data sharing where third-country jurisdiction risks are high. We further support proposals to limit B2G data sharing obligations to public emergencies, and to introduce a lighter cloud switching regime for customised services (concluded before 12 september 2025).

At the same time, we have concerns about specific proposals and how they could be designed or implemented. On biometrics (1-to-1 verification), we are concerned about approaches that create a new exception under Article 9 GDPR; we would instead favor a clarification that 1-to-1 verification falls outside Article 9. On cookies and ePrivacy, we are cautious that proposals promoting automated or machine-readable preference mechanisms. These mechanisms could reduce direct interaction between businesses and users, with potential negative effects—particularly for smaller firms.

We have concerns about the proposal to create a single central EU Single Entry Point platform for incident reporting across cyber and privacy. While intended to streamline reporting, it would increase security and national-security risks by creating a high-value central target. We would instead support a proposal based on one national reporting hub per Member State, with interoperable easy onward transmission – where required - to the relevant competent authorities.

In the following paragraphs we will explain our position in more detail.

I. Our assessment of the Digital Omnibus on AI proposal

AI ACT: Postponement of implementation deadlines high-risk AI

VNO-NCW and MKB-Nederland underwrite the importance of needing to improve implementation periods of new rules. Clarity on how to comply as well as reasonable periods to implement new obligations, is imperative to ensure that rules can be effectively implemented and supported.

Applying a pressure cooker both on the drafting of new laws as well as on the implementation thereof, does not help to meet the intended objectives and only puts an unnecessary burden on businesses working hard to comply with the new rules (in interaction with the existing rules). Let's not kid ourselves, making sense of the complex rules – and interaction with other rules – is not an easy task.

The proposal of the European Commission to postpone the implementation deadlines for high-risk AI systems⁵ is welcome as clarity on how to comply as well

⁵ The entry into application on Article 6(2) and Annex III is postponed maximum until 2 December 2027; and for Article 6(1) and Annex I maximum until 2 August 2028.

as interplay with existing rules, is still lacking, not in the least for SMEs. Realistic implementation deadlines are a prerequisite for correct and timely compliance.

However, the condition triggering applicability on an earlier date if meaningful clarity is provided beforehand (standards, guidance and compliance support tools are ready), contributes to legal uncertainty. We agree that undue delay should be minimized but it is more important to ensure high quality results (standards, guidance and tools) and making sure companies, specifically SMEs, have sufficient time to take stock of the standards, guidelines and tools in order to adequately implement the rules. It would be preferred if the date of application is postponed by a fixed period to provide for the necessary predictability.

AI ACT: Broader legal ground for bias detection and mitigation

The European Commission proposes to broaden the legal ground for processing special categories of personal data for bias detection and mitigation. This broadening of the scope to also detect and mitigate bias in non-high risk AI enables the detection, prevention and mitigation of bias in all AI systems takes into account the existing safeguards and strict conditions included in the AI Act for high-risk AI. See hereunder under the heading 'existing safeguards'. VNO-NCW and MKB-Nederland support the European Commission in its reasoning that bias detection, prevention and correction constitutes a substantial public interest, to protect natural persons from biases' adverse effects, including discrimination.

Although the detection and mitigation of bias is most important in high-risk AI systems, it is good to note that discrimination and other forms of harmful bias is not limited per se to high-risk AI systems. VNO-NCW and MKB-Nederland support that providers and deployers of non-high risk AI *may exceptionally* process specific categories of personal data to detect and mitigate bias if this is necessary to protect natural persons from biases' adverse effects, including discrimination.

Existing safeguards

The AI Act already includes a legal ground⁶ for the processing of special categories of personal data for bias detection and mitigation *for high-risk AI*. This legal ground can only be used exceptionally and subject to appropriate safeguards and is subject to 6 explicit conditions: (a) other data - including synthetic data - is insufficient to detect and mitigate bias; (b) technical limitations on re-use and state-of-the-art security and privacy preserving measures (including pseudonymization) are in place; (c) secure access: including strict controls and documentation of access to the data, avoidance of misuse and only

⁶ Article 9 paragraph 2 sub g GDPR jo article 10 paragraph 5 AI Act

accessible to authorized persons under the obligation of confidentiality; (d) the specific categories of personal data may not be transmitted, transferred or otherwise accessed by other parties (e) the specific categories of personal data must be deleted after purpose of bias detection or mitigating is met; and (f) the strict necessity of processing of the specific categories of personal data needs to be explicitly recorded.

The existing legal ground to process special categories of data is included to enable providers and deployers to meet the obligation of the AI Act (article 10.2) to detect, prevent and mitigate bias that is likely to affect health and safety of persons, have a negative impact on fundamental rights or lead to prohibited discrimination mitigation in training, validation and testing data sets.

AI ACT: AI Literacy

We support the European Commission tasking itself and the Member States to foster AI literacy instead of burdening all companies, large and small, with a disproportionate broad obligation which not seems to be limited to the provision or deployment of high-risk AI. We have been asking our government to include Digital (AI) literacy in the curriculum in the Netherlands for years. We agree with the European Commission that AI literacy should be a strategic priority. AI literacy should not only focus on the work force but on the whole of society. It is therefore important, that the Member States together with the European Commission in a coordinated manner, are tasked with ensuring a sufficient level of AI literacy of all EU citizens. It is important to ensure synergy between MMs and between the Commission and the MMs to prevent fragmentation in the EU.

It is also good to note that article 4 is not the only AI literacy obligation in the AI Act. The important **other** obligation of the AI Act is for providers and deployers to ensure AI literacy of their humans-in-the-loop.⁷ Providers and deployers are required to ensure that persons tasked as human-in-the-loop have the necessary competence, training, authority and necessary support needed to fulfil this task. We underwrite this obligation of the AI Act. However, more guidance is required for companies to fulfil this important task.

AI ACT: Reducing the registration burden

VNO-NCW and MKB-Nederland support the proposal of the European Commission to delete the disproportionate obligation for providers to register AI systems in the EU database under Annex III, in the event their AI systems are not considered a high-risk application of AI. We have advocated for the exemption in article 6(3) AI Act because the Annex III high-risk areas are very broadly defined. It is important that the vast obligations for high-risk AI applications are indeed limited to high-risk AI applications and do not include non-high-risk applications

⁷ Article 26(2) AI Act

in their slipstream. Such as AI applications which are only used for preparatory tasks and where a human does not base its decision solely on this input. For instance, a HR assessment which uses a AI module to determine a person's level of AI literacy. This would fall within the scope of one of the high-risk areas of Annex III (4a). But if the whole selection-assessment includes, besides that one AI component, many face-to-face elements, such as face-to-face discussions, face-to-face interviews, in-person games etc. It would be disproportionate to classify the whole assessment as high-risk AI due to that one AI component.

If we follow the logic of the DPAs, registering of low-risk preparatory AI components need to be registered for them to be able to check whether the assessment has been done right. But do we seriously need a registration of all those non-high risk AI applications, just in case DPAs have the resources and time left to check this? Or do we want the DPAs to focus on truly high-risk applications? Chances are that the majority if not all those registrations will not be used at all by the DPAs. In the context of burden reduction at least such 'just in case' registration requirements for low risk applications of AI need to be deleted.

AI ACT: Extending derogations of micro-enterprises to SMEs

VNO-NCW and MKB-Nederland support the proposal of the European Commission to extend the derogation from micro-enterprises to SMEs to comply with certain elements of the quality management system in a simplified manner. Harmonized and simplified formats, easy to use harmonized online implementation tools as well as proportionality and a risk-based approach are important burden reduction measures for SMEs.

AI ACT: Cooperation competent authorities

VNO-NCW and MKB-Nederland support proposals to strengthen the cooperation between competent authorities to provide each other with mutual assistance necessary for fulfilling their respective mandates, with a view to ensuring coherent application of this Regulation and Union law. It is important that the competent authorities take each other's point of view into account as well as the practical implications for companies of implementing all the complex and interplaying rules.

II. Our assessment of the Digital Omnibus proposal (Data, GDPR and cyber reporting)

Targeted amendments to the GDPR

VNO-NCW and MKB-Nederland welcome targeted amendments to the GDPR which increase the clarity of the provisions, improve the coherence with other

rules of the Digital rulebook, make the rules more predictable, proportionate, risk-based and easier to implement. This will improve the aim of that GDPR, which is to ensure a balance between the free movement of personal data and the protection of privacy.

VNO-NCW and MKB-Nederland encourage the development and adoption of trustworthy AI which is key in providing for economic growth and supporting innovation with socially beneficial outcomes.

GDPR: Definition personal data

VNO-NCW and MKB-NL welcome the effort to clarify that the existence of additional data that could be used to identify the data subject does not in itself imply that pseudonymized data must be considered personal data in all cases and for everyone (to align with the ECJ SRB case). It depends on the means reasonably likely to be used to identify the natural person by the actual recipient(s)⁸.

The proposal of the European Commission confirms that pseudonymization, depending on the circumstances of the case, can effectively prevent persons other than the controller from identifying the data subject in such a way that the data subject is not or no longer identifiable to them.⁹

The proposal does not lower the existing threshold of ‘not having the means’. The recipient is still only considered ‘not to have the means’ when identification of the data subject is prohibited by law or is impracticable in practice, for example because it requires an excessive effort in terms of the time, costs, and manpower required, so that the risk of identification appears negligible in reality.¹⁰

But this proposal has received many reactions, making it clear that the wording of the proposed Article 4 is not clear for everyone. Because clarity is an essential requirement of legal certainty, we suggest to improve the wording to better reflect the meaning of the SRB ruling and to prevent misinterpretation of this key definition.

Specifically smaller controllers need more support with respect to the criteria and means to determine whether data resulting from pseudonymization does not constitute personal data for another person.

⁸ See recital 80 of the ECJ EDPS/SRB ruling: “As the Advocate General observed, in essence, in point 51 of his Opinion, those clarifications relating to the assessment of whether or not the data subject is identifiable would be deprived of any practical effect if pseudonymised data were to be regarded as constituting, in all cases and for every person, personal data for the purposes of the application of Regulation 2018/1725.”; see also recital 82 of the ECJ SRB ruling.

⁹ See recital 87 ECJ SRB ruling

¹⁰ See recital 46 Breyer ECJ ruling

GDPR: Definition scientific research

VNO-NCW and MKB-Nederland also welcome the effort to clarify the definition of *scientific research*. The proposal explicitly confirms that scientific research includes research and technology development (innovation) in academic, industry and other settings such as SMEs. This is the interpretation of scientific research as was initially foreseen by the legislators. The clarification does not alter the requirements for scientific research: research needs to be of high quality and meet the conditions of scientific research, such as methodological and systematic approach. The clarification proposal further clarifies that further processing *for scientific purposes* is compatible with the initial purpose of processing. This clarification is needed because, although it was originally intended to be interpreted as aforementioned, it has not always been interpreted accordingly. It also explicitly clarifies that scientific research constitutes a legitimate interest.¹¹ This is a codification of the ECJ KNLTB ruling¹² in which the European Court of Justice confirmed that all *lawful* interests can in principle be legitimate interests. This is a welcome codification to ensure harmonized interpretation and enforcement across Member States. The GDPR balances the right to protection of personal data, pursuant to Article 8 CFREU, with the freedom of science, pursuant to Article 13 CFREU¹³. The conditions and safeguards of article 89 GDPR remain unchanged. The proposal provides clarity but does not lower the intended protection and purpose of the GDPR, the principles and obligations of the GDPR still need to be taken into account. This is a welcome clarification to ensure harmonized interpretation and enforcement across Member States.

GDPR: Residual traces special categories data

VNO-NCW and MKB-Nederland welcome the clarification in Article 9 regarding the *residual* processing of special categories of personal data in AI training, testing or validation data sets where removal of such data requires *disproportionate* effort. This exemption does not undermine the obligation of the provider of an AI system or model to mitigate risks through appropriate technical and operational measures with regard to the collection and otherwise processing of special categories of personal data. If despite aforementioned measures been taken, residual traces of special categories of personal data appear and the removal of those residual traces requires disproportionate effort, the provider is obligated to undertake effectively technical and operational measures to

¹¹ Article 6(1)(f) GDPR.

¹² ECJ ruling KNLTB vs AP; 4 October 2024, Case C-621/22

¹³ See recital 32 GDPR.

mitigate the risk of those residual traces of special categories of data from further appearing in outputs or otherwise being disclosed. The principles and obligations of the GDPR still need to be taken into account. This proposal provides clarity and is aligned with the aim of the GDPR to ensure a balance between the free movement of personal data and the protection of privacy. Also, it is important to make a distinction between special categories of personal data relating to a public figure and non-public figures. Special categories of personal data and criminal data about public persons may be legitimately included on the basis of article 9.2.g jo article 11 ECHR (freedom of information). For instance, religious beliefs of the pope and political opinions of parliament members.¹⁴

GDPR: Biometric verification

The proposal to include an exemption in article 9 regarding the processing of biometric data for the mere verification of a natural person (one-on-one) raises some questions. The acknowledgement is welcome that the temporary processing of biometric data for the mere confirmation of an individual already known to the controller, is a low risk processing activity. However, in our opinion, an exemption is not needed. History of the GDPR shows that the processing of biometric data for mere verification purposes was not intended to fall within the scope of article 9 GDPR. Therefore, a mere clarification that one-on-one verification falls outside the scope of the ban of article 9 GDPR is sufficient.

In addition, VNO-NCW and MKB-Nederland questions the inserted condition that the biometric data or the means needed for the verification need to be under the sole control of the data subject. Which means that the data subject holds the biometric template or the decryption key to access the template. To ensure that the controller does not gain knowledge of the biometric data, or only for the limited time of the verification process. This is included to prevent further processing of the biometric data (without the active involvement of the data subject). We question whether the requirement - that the data subject holds the biometric template or the decryption key to access the template – is aligned with common secure and accepted practices, such as in high security facilitations. For instance, if verification is needed to gain strict secure access (e.g. nuclear power plant), we question whether it is feasible that the data subject holds the biometric template or the decryption key to access the template.

Instead of an exemption, we would welcome the acknowledgement that verification falls outside the scope of article 9 GDPR. This would also align with the risk based approach of the GDPR, align with the AI Act and be a welcome clarification to ensure harmonized interpretation and enforcement across Member States.

¹⁴ See Case C-507/17, Google LLC vs CNIL et al, 24 September 2019, para 60

GDPR: Legitimate interest – AI

VNO-NCW and MKB-Nederland welcome the explicit clarification that legitimate interest can be a legal ground for processing personal data in the context of the development and operation of an AI system, except where other Union or national laws explicitly require consent. This proposal provides clarity but does not lower the intended protection and purpose of the GDPR. The proposal merely makes explicit that legitimate interest can be used as a legal ground for processing of personal data within the context of the development and operation of AI systems *provided* the legitimate interest of the controller or a third party meets the required 3-step test. Meaning that the interest must be legal and the processing is strictly necessary for the purposes of the legitimate interest in question and that, in the light of all the relevant circumstances, the interests or fundamental rights and freedoms of the data subjects do not override that legitimate interest of the controller (or relevant 3rd party). The other principles and obligations of the GDPR also still need to be taken into account, such as data minimalization, purpose limitation etc. This proposal is a codification of the ECJ KNLTB ruling¹⁵ in which the European Court of Justice confirmed that all *lawful* interests can in principle be legitimate interests. This is a welcome codification to ensure harmonized interpretation and enforcement across Member States. This reassurance is important to build a strong position on trustworthy AI which is key in providing for economic growth and supporting innovation with socially beneficial outcomes. However, VNO-NCW/MKB-NL is concerned about the unconditional right to object¹⁶, which could require halting AI training on a data subject's personal data. This is technically impossible for existing models or inferred data, and retroactive removal would necessitate retraining, which is practically very challenging. VNO-NCW/MKB-NL therefore proposes to clarify that the right to object only applies prospectively.

GDPR: Risk based approach

VNO-NCW and MKB-Nederland welcome the necessary clarification that low-risk processing of personal data requires a less intensive approach than high-risk processing of personal data. This principle of proportionality is made more explicit in the Digital Omnibus proposal regarding the right of access, information requirements and data breach notifications.

¹⁵ ECJ ruling KNLTB vs AP; 4 October 2024, Case C-621/22

¹⁶ Art. 88c as proposed in the Digital Omnibus

GDPR: Abuse of the right of access

VNO-NCW and MKB-Nederland welcome the acknowledgement that in practice the right of access is not always used by data subjects to be granted access to their personal data but instead to be paid a compensation, potentially even under the threat of bringing a claim for damages or offer to withdraw the request in return for compensation. Or situations where data subjects make excessive use of the right of access with the only intent of causing damage or harm to the controller, in particular because of their repetitive character. Such requests place a significant burden on companies, specifically SMEs. It is important that companies can focus their efforts on legitimate access requests.

Within this context, VNO-NCW and MKB-Nederland welcome keeping the burden of proof to a reasonable extent regarding the excessive character of a request. However, specifically SMEs need more guidance (including examples) about what concretely constitutes an 'excessive request'.

GDPR: Information requirements

VNO-NCW and MKB-Nederland support the proposal that information about the processing of personal data does not have to be provided if there are reasonable grounds to expect the data subjects already has that information. For instance, if you rent a car you can expect the rental company to process information about who you are (name and address) and if you have a drivers' license (and for which type of vehicles). For this exemption to kick in, the processing needs to be non-intensive (not complex and low amount of personal data), not likely to result in a high-risk (within the meaning of article 35) and a direct relationship exists between controller and data subject (such as baker, hairdresser, car rental, carpenter, shoemaker or other small retailer, craftsman or local sports club). This exemption benefits small operators, it reduces the disproportionate burden on such small operators in low-risk situations where the processing of personal data is not the core activity of the controller.

VNO-NCW and MKB-Nederland have concerns about the condition that the controller may not transmits the data to other recipients or categories of recipients. A small company or club may under normal circumstances not transmit the data to other recipients but it will always need to comply with legal orders by competent authorities, including the police or a district attorney. VNO-NCW and MKB-Nederland would welcome further clarification that legal orders fall outside the scope of aforementioned condition.

VNO-NCW and MKB-Nederland also welcome the exemption to the information requirement with regard to scientific research. Specifically for the situation where the controller at the time of collection of the personal data did not know that it would process personal data for scientific research purposes at a later stage. The controller may inform data subjects by making the information publicly available in a manner that as many data subjects concerned are reached.

GDPR: Data breach notifications

VNO-NCW and MKB-Nederland welcome the proposal to introduce a higher threshold for data breach notifications to the *competent authority*. It is good to note that the threshold for notification to the data subject remains the same. The proposal requires notifications to the competent authority (Data Protection Authority) only to be submitted if a data breach is likely to result in a high risk to the rights and freedoms of the data subject. This coincides with the instances where a data subject needs to be notified by the controller. This proportionate approach reduces disproportionate notification burdens and enables companies and competent authorities to focus their efforts on data breaches which are likely to result in a high-risk. VNO-NCW and MKB-Nederland also welcome the proposal for a harmonized common template for notifying data breaches, a common (dynamic and non-exhaustive) list of circumstances in which a personal data breach is likely to result in a high risk, as well as the proposal to extend the deadline for data breach notification from 72 to 96 hours. These proposals are specifically helpful for SMEs (they can focus their limited resources on high-risk situations), although they are still required to document all low risk data breaches and the mitigating measures they have undertaken (in case a DPA asks for this).

GDPR: Data Protection Impact Assessment (DPIA)

VNO-NCW and MKB-Nederland welcome a harmonized list of processing activities that require a DPIA, a harmonized list of common processing activities which do not require a DPIA as well as a harmonized template and methodology for conducting a DPIA and subsequent reporting. This would bring necessary clarification and harmonization about an obligation which requires a lot of resources, specifically of SMEs.

e-Privacy Directive & GDPR: Cookies and similar techniques

VNO-NCW and MKB-Nederland have been asking for a solution for the consent fatigue for a long time. The interplay between the e-Privacy directive¹⁷ and the

¹⁷ Article 5(3) of the ePrivacy directive, 2002/58/EC on privacy and electronic communications

GDPR increases the complexity for companies.

The ePrivacy Directive applies to the placement of cookies or similar technologies to gain information from a user's terminal equipment, while the subsequent processing of personal data is subject to the GDPR. Under the ePrivacy Directive consent is the required legal basis for cookies but the legal processing grounds for the subsequent processing can be one of the 5 other legal grounds of the GDPR. For instance, necessity for the performance of a contract.

The complexity of the interplay between these 2 pieces of legislation has led to legal uncertainty and subsequent higher compliance costs. In addition, in some Member States, such as in the Netherlands, two different national authorities are tasked with the supervision of the different rules and two different ministries are responsible for the different legal frameworks.

VNO-NCW/MKB-Nederland welcome the efforts to simplify the interplay of the rules on cookies (and similar technologies) and possible subsequent processing of personal data. We support the proposal that processing of personal data on and from terminal equipment will be governed only by the GDPR. We also support that the ePrivacy Directive will remain applicable for connected devices of legal persons and the use of cookies (and similar techniques) pertaining to non-personal data if and in so far necessary to protect the confidentiality of communication on public electronic communication networks.

However, we have concerns about consent as the sole legal processing ground for accessing terminal equipment of a natural person when personal data is collected.

Notwithstanding that the proposed amendments provide for certain exemptions where it should not be necessary to obtain consent and where the subsequent processing should be considered lawful, in particular where they pose a low risk to the rights and freedoms of the data subjects or where the placement of such technologies is necessary for the provision of a service requested by the data subject, this does not provide for other instances where consent is also not the proper legal processing ground. For instance, consent is not the proper legal processing ground with regard to the employee-employer relationship if the processing activity is not solely beneficial for the employee. For example, an employer needs to be able to control its internal communication systems, including terminal equipment, in the event of grounded suspicion of fraud or corporate espionage. It is therefore necessary to be able to apply the most appropriate legal processing ground depending on the purpose of a given processing activity.

In addition, VNO-NCW and MKB-Nederland has concerns about the proposal paving the way for automated and machine-readable indications of individual choices. This, again, does not take into account that consent is not the only proper legal processing ground; and the possibility of making automated choices is not per se granular. Being able to efficiently and effectively advertise for products and services is an important marketing tool for all companies, big and small. VNO-NCW and MKB-Nederland stress the importance of the possibility for individuals to choose from which specific (trusted) company they would (or not) like to receive (tailored and contextual) advertisements. The proposal seems to support the possibility of granular choices where they refer to agentic AI as support tool for persons in making specific consent choices. But, the possibility of granular choices needs to be the default proposition where consent is the proper legal processing ground, to allow for direct interaction between companies and its (prospective) customers. . To truly battle consent fatigue, it is important to allow for all 6 legal processing grounds of the GDPR. It is also important to take into consideration that there is no strict hierarchy between the six legal grounds for processing personal data.¹⁸

In addition, VNO-NCW/MKB-Nederland is concerned about the requirement that a company may not ask for consent again within a time period of 6 months. This is a long period and would entail the storage of personal data (the refusal) for at least six months.

NIS, CER, CRA and GDPR: Single Entry Point (Cybersecurity and Data Breach incidents)

VNO-NCW and MKB-Nederland are not in favor of a single central reporting platform at the European level. VNO-NCW and MKB-Nederland would support a single reporting platform at the national level.

For the majority of companies based in the Netherlands and covered by NIS2 or CER there is little or no efficiency gain in a SEP on European level. More importantly, VNO-NCW and MKB-Nederland has concerns about the security of a European central platform and database. This might prove an attractive target for criminals, state actors, etc. In short, a risk to national security.

VNO-NCW and MKB-Nederland supports a single reporting platform at Member state (national) level. The EC or ENISA could possibly provide/draw up guidelines for this. In the Netherlands, the necessary steps are being taken to set up a single reporting platform at national level: reports from NIS2, CER, CRA, and Netcode will soon all be able to be reported to the National Cyber Security Center (NCSC). The NCSC will subsequently forward them to the supervisory

¹⁸ See Opinion of Advocate General Szpunar in Case C-394/23, Mousse (ECLI:EU:C:2024:610), para 28

authorities. VNO-NCW and MKB-Nederland support using the same point for reporting Data breaches under the GDPR.

Data access and sharing

Consolidation data rules

VNO-NCW and MKB-Nederland support the efforts to consolidate the EU data rules¹⁹ in the Data Act. Coherence between the different rules of the digital rulebook is a prerequisite for clarity and subsequent legal certainty. However, further proposals would be welcome to ensure coherence between aforementioned data rules and the GDPR.

VNO-NCW and MKB-Nederland support the proposals to facilitate the economic viability and growth of data intermediation services providers. To this end, we concur that the obligation to keep data intermediation services legally separate from any other service a company may want to offer, is a problematic obligation in terms of economic viability. VNO-NCW and MKB-Nederland support the proposal to replace this troublesome obligation with the obligation to solely keep the different services functionally separate. VNO-NCW and MKB-Nederland also support the proposal to drastically shorten the list of obligations.

Data Act: Trade secrets

VNO-NCW and MKB-Nederland support the proposal to further strengthen the trade secrets protection in the Data Act. In the context of improving our resilience, the proposal to include the possibility for data holders to refuse data sharing requests if this poses a high risk of unlawful acquisition, use, or disclosure to third country entities that are subject to jurisdictions with weaker protections than those available in the Union. However, for companies it might not always be possible to provide the necessary proof of such high-risk, specifically for smaller companies. It should therefore not be required of individual companies to undertake a costly assessment of international law and practices. Refusing a data sharing request should be possible on the basis of general knowledge. VNO-NCW and MKB-Nederland also request the inclusion of an obligation for the European Commission and Member States to provide general assistance (e.g. adequacy decisions). It is not realistic to require SMEs to conduct extensive third-country-law analyses.

Data Act: B2G data sharing

VNO-NCW and MKB-Nederland support the proposal to narrow the scope of

¹⁹ Free Flow of Non-personal Data Regulation, Data Governance Act, the Open Data Directive and Data Act.

chapter 5 (B2G data sharing) of the Data Act to public emergencies (instead of exceptional needs). Governments can request data from companies when necessary to respond to a public emergency or to mitigate or support the recovery from a public emergency

Data Act: Cloud switching

VNO-NCW and MKB-Nederland support the proposed lighter regime for switching between cloud service providers when custom made cloud service are provided and the contract is concluded before 12-9-25 and the term custom build is not too broadly interpreted. Custom made cloud services are data processing services that are not off-the-shelf and would not function without prior adaptation to the specific needs and system of the user. VNO-NCW and MKB-Nederland also support the exemption for SMEs (and SMCs) cloud service providers when the contract was concluded before 12-9-25; as well as the clarification that these providers can include early-termination penalties in fixed-term contracts.

Irvette Tempelman
VNO-NCW/MKB-Nederland
[REDACTED]@vnoncw-mkb.nl

Bijlage 1 -

Guidance under preparation by the Commission include:

- Guidelines on the practical application of the high-risk classification;
- Guidelines on the practical application of the transparency requirements under Article 50 AI Act;
- Guidance on the reporting of serious incidents by providers of high-risk AI systems;
- Guidelines on the practical application of the high-risk requirements; Guidelines on the practical application of the obligations for providers and deployers of high-risk AI systems;
- Guidelines with a template for the fundamental rights impact assessment;
- Guidelines on the practical application of rules for responsibilities along the AI value chain;
- Guidelines on the practical application of the provisions related to substantial modification;
- Guidelines on the post-market monitoring of high-risk AI systems;
- Guidelines on the elements of the quality management system which SMEs and SMCs may comply with in a simplified manner;
- Guidelines on the AI Act's interplay with other Union legislation, for example joint guidelines of the Commission and European Data Protection Board on the interplay of the AI Act and EU data protection law, guidelines on the interplay between the AI Act and the Cyber Resilience Act, and guidelines on the interplay between the AI Act and the Machinery Regulation;
- Guidelines on the competences and designation procedure for conformity assessment bodies to be designated under the AI Act.

Irvette Tempelman

VNO-NCW/MKB-Nederland

5.2.1 [redacted]@vnoncw-mkb.nl