

Nr. . Verslag van de Rapporteurs van de Eerste Kamer

Vastgesteld op ..mei 2026

Inleiding

De Europese Commissie heeft op 19 november 2025 het zogeheten ‘Digitaal pakket’ ingediend, waaronder twee wetgevende initiatieven vallen: de Omnibus AI en de Omnibus Digitaal (zie het kader hieronder voor een toelichting op deze voorstellen).

In de Eerste Kamer zijn de leden Mary Fiers (GroenLinks-PvdA) en Van de Sanden (Fractie-Van de Sanden) benoemd tot rapporteur bij de behandeling van de voorstellen Omnibus AI en Omnibus Digitaal. Doel van het rapporteurschap is het verbeteren van de informatiepositie van de Eerste Kamer op deze voorstellen.¹ Hiertoe hebben de rapporteurs in afstemming met hun commissies al een aantal acties geïnitieerd. In mei 2026 is samen met de rapporteurs El Boujdaini (D66) en Van den Berg (JA21) in de Tweede Kamer een eerste verslag aangeboden over een gezamenlijk werkbezoek aan Brussel.¹ In dit tweede verslag wordt ingegaan op vier gesprekken die hebben plaatsgevonden met wetenschappers, maatschappelijke organisaties, toezichthouders en vertegenwoordigers van het bedrijfsleven. Deze gesprekken hadden tot doel de belangrijkste aandachtspunten, risico's en mogelijke knelpunten rondom de Omnibus AI en de Omnibus Digitaal in kaart te brengen.

In Bijlage 1 brengen de rapporteurs verslag uit over de volgende gevoerde gesprekken:

1. Op 28 april 2026 vond een gesprek plaats met wetenschappers van de Open Universiteit en de Universiteit van Amsterdam over 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.

¹ *Kamerstukken I*, 2025/2026, 36.890, F.

2. Op 29 april 2026 vond een gesprek plaats met maatschappelijke organisaties en vertegenwoordigers van grondrechtenorganisaties over de gevolgen van de voorstellen voor de bescherming van grondrechten, waaronder privacy, gegevensbescherming en non-discriminatie. Aan dit gesprek namen vertegenwoordigers van Bits of Freedom, het College voor de Rechten van de Mens en Stichting Data Bescherming Nederland deel.
3. Op 29 april 2026 vond daarnaast een gesprek plaats met nationale toezichthouders over de gevolgen van de voorstellen voor toezicht, uitvoerbaarheid en handhaafbaarheid. Daarbij werd specifiek gesproken over de rol en capaciteit van de Autoriteit Persoonsgegevens (AP) en de Autoriteit Consument en Markt (ACM), alsmede over mogelijke knelpunten in de uitvoering en coördinatie van toezicht.
4. Tot slot vond op 13 mei 2026 een gesprek plaats met vertegenwoordigers van het Adviescollege Toetsing Regeldruk (ATR) en VNO-NCW over de huidige en verwachte regeldruk voor bedrijven en de mogelijke effecten van de voorstellen op concurrentiekracht, uitvoerbaarheid en lastenverlichting.

De Omnibus AI (COM (2025)836) moet volgens de Europese Commissie de toepassing van de AI-verordening vereenvoudigen en administratieve lasten voor bedrijven verminderen, terwijl de kern van het risico gebaseerde AI-kader behouden dient te blijven. De Commissie presenteert het voorstel als onderdeel van haar bredere agenda om de Europese concurrentiekracht, innovatiecapaciteit en ontwikkeling van AI in Europa te versterken. Een van de belangrijkste onderdelen betreft het uitstel van verplichtingen voor hoog-risico-AI-systemen.

De Omnibus Digitaal (COM (2025)837) beoogt bestaande Europese digitale wetgeving op het gebied van data, AI, privacy, platforms en cyberveiligheid te vereenvoudigen en beter op elkaar af te stemmen. De Europese Commissie wil hiermee overlap in regels, dubbele rapportage- en nalevingsverplichtingen en verschillen tussen sectorale regels verminderen, zodat het digitale regelgevingskader consistent, beter uitvoerbaar en minder belastend wordt voor bedrijven en toezichthouders.

Kernpunten

Een eerste terugkerend punt betrof de gevolgde omnibusprocedure. Alle gesprekspartners wezen er vanuit verschillende invalshoeken op dat omnibuswetgeving uitsluitend is bedoeld voor technische aanpassingen, verduidelijkingen of administratieve lastenverlichting. Verschillende voorgestelde wijzigingen gaan echter volgens deskundigen verder dan dat. Dit geldt in het bijzonder voor de wijziging van de definitie van persoonsgegevens in de AVG, de nieuwe bepalingen over het gebruik van bijzondere persoonsgegevens voor AI-training en de aanpassing van waarborgen rond geautomatiseerde besluitvorming.

In alle gesprekken werd benadrukt dat het ontbreken van een formeel impact assessment de parlementaire beoordeling bemoeilijkt, omdat de gevolgen van de wijzigingen niet goed zijn onderzocht. De AP kwalificeerde het Staff Working Document van de Europese Commissie als te algemeen en oppervlakkig om als alternatief voor een impact assessment te kunnen dienen. Ook ATR en VNO-NCW benadrukten dat bij een omvangrijk pakket met uiteenlopende wijzigingen inzicht nodig is in de feitelijke gevolgen voor uitvoerbaarheid, regeldruk en naleving. Daarbij werd door VNO-NCW specifiek gewezen op de triloofase, waarin in de praktijk vaak substantiële wijzigingen worden aangebracht zonder dat de gevolgen daarvan opnieuw worden getoetst.

Wetenschappers wezen daarbij ook op een mogelijke juridische kwetsbaarheid van de gekozen route: indien later zou blijken dat de Commissie niet de juiste procedure heeft gevolgd of buiten haar bevoegdheden is getreden, kan dit gevolgen hebben voor de geldigheid van de uiteindelijke regelgeving. Daarbij werd benadrukt dat procedures bij het Hof van Justitie van de Europese Unie lang kunnen duren, terwijl feitelijke gevolgen van de regelgeving zich in de tussentijd mogelijk moeilijk laten terugdraaien.

In meerdere gesprekken werd daarnaast benadrukt dat de Omnibusvoorstellen niet noodzakelijk leiden tot de door de Commissie beoogde vereenvoudiging. Stichting Data Bescherming Nederland gaf bijvoorbeeld aan aanvankelijk positief te hebben gestaan tegenover het doel om digitale regelgeving te verduidelijken en te vereenvoudigen, maar stelde dat de Omnibus Digitaal op verschillende onderdelen juist nieuwe juridische onzekerheid lijkt te creëren, onder andere door begrippen te breed of onvoldoende precies te formuleren. Ook de AP wees erop dat de AI-verordening nog niet volledig is ingevoerd, terwijl nu al wijzigingen worden voorgesteld. Dit kan volgens de AP leiden tot extra complexiteit, rechtsonzekerheid en uitvoeringsproblemen. VNO-NCW steunt daarentegen de voorgestelde aanpassingen van de AVG. Bedrijven hebben last van de verschillen in de uitleg van de AVG tussen de toezichthouders in de verschillende lidstaten. De voorgestelde wijzigingen worden door VNO-NCW slechts als 'babystapjes' gezien om de AVG meer proportioneel te maken voor het bedrijfsleven.

Een centraal inhoudelijk punt betrof de voorgestelde wijziging van het begrip ‘persoonsgegevens’ in de AVG. Wetenschappers, maatschappelijke organisaties en de AP wezen erop dat dit begrip de toegangspoort vormt tot de bescherming van de AVG. De Europese Commissie presenteert de wijziging mede als codificatie van jurisprudentie van het Hof van Justitie van de Europese Unie, maar meerdere gesprekspartners betoogden dat het voorstel verder gaat dan louter codificatie. In de gesprekken werd vooral gewezen op de contextafhankelijke beoordeling van gepseudonimiseerde gegevens: gegevens kunnen voor de ene partij wel en voor de andere partij niet als persoonsgegevens kwalificeren, afhankelijk van de middelen waarover die partij beschikt om betrokkenen te identificeren. Volgens wetenschappers kan dit juist voor wetenschappelijk onderzoek rechtsonzekerheid vergroten, omdat partijen uit voorzorg geneigd zullen zijn gepseudonimiseerde gegevens als persoonsgegevens te behandelen.

Ook de voorgestelde bepalingen over het gebruik van bijzondere persoonsgegevens voor het trainen van AI-systemen vormden een belangrijk gesprekspunt. Daarbij werd het belang van toegang tot data voor AI-ontwikkeling erkend, maar ook gewezen op de risico’s voor privacy en non-discriminatie. Bits of Freedom en Stichting Data Bescherming Nederland vrezen dat de voorstellen de verwerking van bijzondere persoonsgegevens verder vergemakkelijken, terwijl burgers vaak niet weten in welke datasets hun gegevens voorkomen en hun rechten daardoor moeilijk kunnen uitoefenen.

Daarnaast wezen Bits of Freedom en Stichting Data Bescherming Nederland op de voorgestelde wijziging van artikel 22 AVG over geautomatiseerde besluitvorming. Volgens hen kan deze wijziging het eenvoudiger maken om AI-systemen in te zetten bij besluiten over burgers. Daarbij waarschuwden zij dat fouten of bias zich niet incidenteel, maar structureel en op grote schaal kunnen herhalen. Daarbij werd benadrukt dat een *human in the loop* niet vanzelfsprekend voldoende bescherming biedt. Alleen wanneer een medewerker daadwerkelijk beschikt over voldoende informatie, tijd en autonomie om van een systeemuitkomst af te wijken, kan sprake zijn van betekenisvolle menselijke tussenkomst.

Een ander besproken onderdeel betrof het inzagerecht onder de AVG. Wetenschappers wezen erop dat de Omnibus Digitaal het inzagerecht inperkt door sterker te benadrukken dat dit recht moet worden gebruikt om de rechtmatigheid van gegevensverwerking te controleren. Daarbij werd opgemerkt dat in de Nederlandse rechtspraak al situaties bestaan waarin misbruik van het inzagerecht kan worden aangenomen als een verzoek voor een ander doel wordt gedaan. Hierover bestond wel een meningsverschil tussen de verschillende wetenschappers. Enerzijds gaf een van de wetenschappers aan dat het prima was dat de EC dit opnam, dit stond namelijk al vermeld in overweging 63 van de AVG. Anderzijds werd door sommige wetenschappers betwijfeld of de Europese

Commissie voldoende heeft onderbouwd dat misbruik van het inzagerecht zich op zodanige schaal voordoet dat een sterkere benadrukking gerechtvaardigd is. Ook werd door de wetenschappers gewezen op mogelijke gevolgen voor wetenschappelijk onderzoek, omdat betrokkenen hun inzagerecht soms gebruiken om gegevens beschikbaar te krijgen voor deelname aan onderzoek.

Onder andere de wetenschappers, maatschappelijke organisaties en de AP uitten ook zorgen over het oorspronkelijke voorstel om de verplichting tot AI-geletterdheid voor aanbieders en gebruiksverantwoordelijken af te zwakken en te verschuiven naar een bredere bevorderingsplicht voor lidstaten en de Europese Commissie. Volgens hen neemt dit een belangrijke prikkel weg voor organisaties om te investeren in kennis en vaardigheden van medewerkers, terwijl AI-geletterdheid juist nodig is om risico's voor burgers, werknemers en grondrechten te herkennen.

Als laatste kwam toezicht en handhaafbaarheid in meerdere gesprekken naar voren. Zo was de AP kritisch op de voorgestelde verhoging van de meldingsdrempel bij datalekken, omdat organisaties risico's in de praktijk regelmatig onderschatten. Het College voor de Rechten van de Mens, Bits of Freedom en Stichting Data Bescherming Nederland waarschuwden daarnaast dat een wijziging van de registratieplicht kan ertoe leiden dat systemen die feitelijk als hoog risico moeten worden aangemerkt, niet als zodanig zichtbaar worden in de Europese databank. Dat kan het toezicht bemoeilijken en de transparantie voor betrokkenen verminderen. Het College voor de Rechten van de Mens wees op de mogelijke beperking van bevoegdheden van grondrechtenautoriteiten onder de AI-verordening. Wanneer zij documentatie over hoog-risico-AI-systemen niet langer zelfstandig kunnen opvragen, kan dit volgens het College de effectiviteit van toezicht op grondrechtenrisico's beperken.

Bijlage 1: Gespreksverslagen

De gesprekken vormen nadrukkelijk een aanvulling of toelichting op de position papers.

Gespreksverslag wetenschappers (Open Universiteit en Universiteit van Amsterdam)

Tijdens het gesprek met wetenschappers van de Open Universiteit en de Universiteit van Amsterdam werd stilgestaan bij de Omnibusprocedure, de bescherming van grondrechten en rechts(on)zekerheid. Ook werd uitgebreid stilgestaan bij de impact van de Omnibusvoorstellen op de rol van wetenschappelijk onderzoek.

De Omnibusprocedure

De wetenschappers uitten kritiek op de gevolgde Omnibusprocedure. Zij benadrukten dat Omnibuswetgeving in beginsel is bedoeld voor technische wijzigingen en niet voor substantiële wijzigingen van het digitale acquis. Volgens hen gaan verschillende voorgestelde wijzigingen, anders dan de Europese Commissie stelt, aanzienlijk verder dan louter technische aanpassingen. Zo wordt in het voorstel van de Europese Commissie de definitie van persoonsgegevens in de AVG gewijzigd, terwijl deze definitie het fundament vormt van de gehele verordening. Daarnaast merkten zij op dat bepaalde voorgestelde wijzigingen van de AVG, anders dan door de Europese Commissie wordt betoogd, veel verder gaan dan een codificatie van arresten van het Hof van Justitie van de Europese Unie (HvJEU). De wetenschappers gaven aan niet op voorhand afwijzend te staan tegenover dergelijke inhoudelijke wijzigingen, maar benadrukten dat deze langs de reguliere wetgevingsprocedure tot stand zouden moeten komen. Voor deze vergaande wijzigingen zou een formeel impact assessment moeten worden uitgevoerd met voldoende aandacht voor de bescherming van grondrechten.

Voorts wezen deze wetenschappers op de mogelijke juridische kwetsbaarheid van de uitkomst van de procedure. Indien het HvJEU op een later moment zou oordelen dat de Europese Commissie niet de juiste procedure heeft gevolgd of buiten haar bevoegdheden is getreden, bestaat het risico dat de Omnibusvoorstellen ongeldig worden verklaard. Daarbij werd gewezen op het feit dat dergelijke procedures bij het HvJEU doorgaans jarenlang kunnen duren, terwijl bepaalde feitelijke gevolgen zich mogelijk niet meer laten terugdraaien.

Het begrip ‘persoonsgegevens’

Tijdens het gesprek werd uitgebreid stilgestaan bij de wijziging van definitie van ‘persoonsgegevens’ van de AVG. De wetenschappers lichtten toe dat deze wijziging deels kunnen worden gezien als een codificatie van jurisprudentie van het HvJEU, maar op onderdelen verder lijkt te gaan.

In het voorstel van de Europese Commissie wordt de kwalificatie van gegevens als persoonsgegevens gelinkt aan de technologische mogelijkheden waarover een verkrijger van gepseudonimiseerde persoonsgegevens beschikt om de identiteit van de betrokkene te achterhalen. De wetenschappers schetsen in dit verband de situatie waarin een verwerkingsverantwoordelijke persoonsgegevens pseudonimiseert en deze vervolgens verstrekt aan een andere organisatie. Indien de ontvangende organisatie de identiteit van de betrokkene redelijkerwijs niet kan achterhalen, worden deze gegevens voor die organisatie onder de huidige AVG niet als persoonsgegevens aangemerkt. Uit de rechtspraak van het Hof van Justitie volgt dat, wanneer een daaropvolgende verkrijger de identiteit van de betrokkene wél kan achterhalen, ook de eerdere ontvanger de gegevens als persoonsgegevens dient te behandelen. Volgens het voorstel van de Europese Commissie zou dat worden afgeschaft.

Volgens de wetenschappers is dit problematisch, omdat partijen uit voorzorg geneigd zullen zijn gepseudonimiseerde gegevens als persoonsgegevens te behandelen, ook wanneer zij zelf de betrokkene redelijkerwijs niet kunnen identificeren. De wetenschappers benadrukten dat dit naar verwachting niet zozeer een belemmering vormt voor grote technologiebedrijven, maar met name nadelige gevolgen kan hebben voor wetenschappelijk onderzoek. Indien pseudonimisering juridisch onzekerder of risicovoller wordt, bestaat het risico dat bepaald onderzoek minder vaak zal worden uitgevoerd.

Gebruik bijzondere persoonsgegevens voor trainen AI

In de Omnibus Digitaal wordt het voorstel gedaan voor het creëren van een grondslag voor het verwerken van bijzondere persoonsgegevens voor het trainen van AI-systemen. Een van de wetenschappers merkte op dat hier wat voor te zeggen valt, nu de AVG in de praktijk regelmatig wordt genoemd als belemmering voor de ontwikkeling en training van AI-systemen. Tegelijkertijd benadrukte de wetenschapper dat de AVG een wezenlijke functie vervult bij bescherming van persoonsgegevens van burgers. Daarmee bestaat op dit punt een belangrijk spanningsveld tussen innovatie en gegevensbescherming.

Een andere wetenschapper wees erop dat het begrip ‘bijzondere persoonsgegevens’ in de jurisprudentie van het HvJEU steeds ruimer wordt uitgelegd. Daardoor komen steeds meer categorieën gegevens onder het strengste beschermingsregime van de AVG te vallen. Deze wetenschapper merkte op dat gegevensbescherming een recht is dat moet worden afgewogen tegen andere relevante belangen. De ontwikkeling van AI binnen Europa is daarbij ook een belang.

Wetenschappelijk onderzoek en misbruik van inzagerecht

De wetenschappers merken op dat het inzagerecht van de AVG, dat betrokkenen in staat stelt zich van de verwerking van hun gegevens op de hoogte te stellen en de rechtmatigheid daarvan te controleren, door de Omnibus Digitaal wordt ingeperkt.

Onder de huidige AVG hoeven betrokkenen een verzoek om inzage niet te motiveren: verwerkingsverantwoordelijken dienen de gevraagde gegevens te verstrekken wanneer een betrokkene daarom verzoekt. Met de Omnibus Digitaal wordt dit gewijzigd: het inzagerecht zal uitsluitend kunnen worden aangewend met het oog op het controleren van de rechtmatigheid van de verwerking van persoonsgegevens, en niet voor andere doeleinden.

Een van de wetenschappers merkte op dat er in Nederland enkele rechterlijke uitspraken bestaan waarin is geoordeeld dat er sprake kan zijn van misbruik van recht wanneer een inzageverzoek wordt gedaan met een ander doel dan controleren van de rechtmatigheid van de verwerking van persoonsgegevens. Daarbij wees de wetenschapper op overweging 63 van de AVG, waarin reeds is opgenomen dat het inzagerecht alleen ertoe strekt om de rechtmatigheid van gegevensverwerking te controleren. Deze wetenschapper zag dan ook geen principiële bezwaren tegen het expliciet opnemen van deze overweging in de bepalingen van de AVG.

Een andere wetenschapper plaatste daarentegen vraagtekens bij de proportionaliteit van de inperking van het inzagerecht. Daarbij werd opgemerkt dat de Europese Commissie geen bewijs heeft gepresenteerd waaruit blijkt dat misbruik van inzagerecht zich op zodanige schaal voordoet dat inperking is gerechtvaardigd. Ook werd gewezen op de mogelijke negatieve gevolgen voor wetenschappelijk onderzoek. In de praktijk oefenen burgers hun inzagerecht wel eens uit om hun gegevens beschikbaar te kunnen stellen aan onderzoek. Dit is straks niet meer mogelijk.

AI-geletterdheid

Ten aanzien van AI-geletterdheid werd opgemerkt dat dit een van de weinige verplichtingen uit de AI-verordening is die ook geldt voor toepassingen die niet als hoog-risico AI-systemen kwalificeren. De Europese Commissie stelt voor om deze verplichting te schrappen voor aanbieders en gebruiksverantwoordelijken van AI-systemen. In plaats hiervan komt een verplichting voor lidstaten en de Europese Commissie om AI-geletterdheid te bevorderen. Door deze verplichting voor bedrijven te schrappen of af te zwakken, wordt volgens een van de wetenschappers een belangrijke prikkel weggenomen om te investeren in de AI-geletterdheid van werknemers.

Dit werd door een van de wetenschappers om meerdere redenen als onwenselijk aangemerkt. In de eerste plaats kan een gebrek aan AI-geletterdheid risico's opleveren voor burgers. Werknemers die AI-systemen gebruiken, moeten in voldoende mate begrijpen hoe deze systemen functioneren, welke beperkingen daaraan verbonden zijn en welke gevolgen het gebruik daarvan kan hebben. Zonder deze kennis bestaat het risico dat AI-systemen onjuist of onzorgvuldig worden ingezet, met alle gevolgen van dien. In de tweede plaats kan het nadelige gevolgen hebben voor de werknemers zelf. Zij moeten wel mee kunnen met de technologie om hun positie op de arbeidsmarkt te

behouden. Tegen die achtergrond benadrukte een van de wetenschappers dat Europa juist stevig zou moeten investeren in AI-geletterdheid.

Wie profiteert?

Ten aanzien van de vraag welke partijen het meest profiteren van de voorgestelde wijzigingen, werd opgemerkt dat het te simplistisch is om te stellen dat uitsluitend grote technologiebedrijven voordeel zullen ondervinden van de Omnibusvoorstellen. Ook het MKB zal baat hebben bij bepaalde onderdelen, bijvoorbeeld bij de voorgestelde wijzigingen rond de meldplicht voor datalekken en andere procedurele vereenvoudigingen die zorgen voor een administratieve lastenverlichting.

Gespreksverslag maatschappelijke organisaties (College voor de Rechten van de Mens, Stichting Data Bescherming Nederland en Bits of Freedom)

Tijdens het gesprek met het College voor de Rechten van de Mens, Stichting Data Bescherming Nederland en Bits of Freedom stonden vooral de gevolgen van de Omnibus AI en de Omnibus Digitaal voor grondrechten centraal, waaronder het recht op privacy en non-discriminatie. De organisaties uitten zorgen over mogelijke verzwakking van het bestaande beschermingsniveau voor burgers.

De Omnibusprocedure

Stichting Data Bescherming Nederland merkte op dat zij aanvankelijk positief tegenover het voornemen stonden om bestaande wetgeving op het digitale terrein te verduidelijken en te vereenvoudigen. Volgens Stichting Data Bescherming Nederland leidt de Omnibus Digitaal echter niet tot de beoogde verduidelijking. Integendeel, de voorstellen lijken op verschillende onderdelen juist meer juridische onzekerheid te creëren dan zij wegnemen. Daarbij werd opgemerkt dat juridische onzekerheid voor de meeste ondernemingen een negatieve impact heeft, terwijl grote ondernemingen dergelijke onzekerheid in de praktijk juist kunnen benutten om juridische procedures te vertragen of onder boetes uit te komen.

De gesprekspartners merkten op dat het begrijpelijk is dat de Europese Unie wil inzetten op innovatie en administratieve lasten wil verlagen en regelgeving wil vereenvoudigen, maar deze exercitie zou niet mogen neerkomen op afzwakking van het beschermingsniveau van de grondrechten van burgers. Zij waren kritisch over de snelheid waarmee Omnibusvoorstellen worden behandeld. Ook werd benadrukt dat maatschappelijke organisaties, toezichthouders en wetenschappers voldoende betrokken moeten blijven bij de ontwikkeling van digitale regelgeving. Volgens hen is brede maatschappelijke betrokkenheid noodzakelijk voor het draagvlak van digitale regelgeving.

Het begrip 'persoonsgegevens'

Tijdens het gesprek is stilgestaan bij de wijzigingen in de AVG, waaronder definities van persoonsgegevens. De gesprekspartners spraken daarbij hun zorgen uit dat deze wijzigingen kunnen leiden tot een lager beschermingsniveau van de grondrechten van burgers en tot meer rechtsonzekerheid.

Bits of Freedom en Stichting Data Bescherming Nederland benadrukten dat het begrip ‘persoonsgegevens’ van fundamenteel belang is, omdat dit begrip bepaalt of de AVG van toepassing is of niet. Daarbij wezen zij erop dat dezelfde gepseudonimiseerde gegevens onder de door de Europese Commissie voorgestelde definitie bij de ene verwerkingsverantwoordelijke niet als persoonsgegevens worden aangemerkt, terwijl dat bij de andere verwerkingsverantwoordelijke wel het geval kan zijn. Dit hangt af van de technologische mogelijkheden waarover de betreffende verwerkingsverantwoordelijke beschikt om de identiteit van de betrokkene te achterhalen. Volgens Bits of Freedom en Stichting Data Bescherming Nederland maakt deze benadering de toepassing en handhaving van de AVG aanzienlijk complexer.

Bits of Freedom en Stichting Data Bescherming Nederland benadrukten daarbij dat persoonsgegevens ruim beschermd moeten blijven, juist omdat technologische ontwikkelingen steeds meer mogelijkheden bieden om personen indirect te identificeren.

Gebruik bijzondere persoonsgegevens voor trainen AI

Tijdens het gesprek werd voorts stilgestaan bij de voorgestelde grondslag voor het verwerken van bijzondere persoonsgegevens voor het trainen van AI-systemen. Onder de huidige AVG is de verwerking van bijzondere persoonsgegevens in beginsel verboden. Bits of Freedom en Stichting Data Bescherming Nederland wezen erop dat in Nederland verschillende voorbeelden bekend zijn waarbij algoritmische systemen een discriminerende uitwerking hadden, mede doordat er bijzondere persoonsgegevens in het systeem waren verwerkt. Tegen deze achtergrond spraken zij hun zorgen uit over de voorgestelde wijziging in de Omnibus Digitaal. Ondanks de bestaande risico's zou het door deze wijziging eenvoudiger worden om bijzondere persoonsgegevens te verwerken. Zo wordt het mogelijk om deze gegevens alsnog te gebruiken voor het trainen van AI-modellen wanneer het te omslachtig wordt geacht om deze gegevens uit een dataset te halen.

Volgens Bits of Freedom en Stichting Data Bescherming Nederland wordt daarmee de deur opengezet voor mogelijke schendingen van fundamentele rechten, enkel om het gemak van verwerkingsverantwoordelijken te dienen. Daarbij merkten zij op dat burgers weliswaar formeel bezwaar kunnen maken tegen het gebruik van hun gegevens, maar dat zij in de praktijk vaak niet weten in welke datasets hun gegevens zijn verwerkt. Daardoor kunnen zij hun rechten niet effectief uitoefenen. Bovendien kunnen persoonsgegevens niet gemakkelijk uit grote taalmodellen worden verwijderd zonder het

model als geheel tot in de kern aan te tasten. Dit ondermijnt de effectieve uitoefening van het recht op vergetelheid.

Geautomatiseerde besluitvorming

Bits of Freedom en Stichting Data Bescherming Nederland merkten op dat de voorgestelde wijziging van artikel 22 AVG het voor organisaties makkelijker zal maken om AI-systemen te gebruiken voor het nemen van geautomatiseerde beslissingen. Onder de huidige AVG is volledig geautomatiseerde besluitvorming slechts bij hoge uitzondering toegestaan en alleen wanneer aan strikte voorwaarden wordt voldaan. De Omnibus Digitaal verruimt deze mogelijkheid. Dit is zorgelijk volgens Bits of Freedom en Stichting Data Bescherming Nederland. Fouten of bias in AI-systemen kunnen ertoe leiden dat discriminatie niet incidenteel blijft zoals bij menselijke besluitvorming, maar zich herhaaldelijk voordoet en daardoor dezelfde groepen burgers structureel en op grote schaal raakt.

Daarbij werd opgemerkt dat een zogenoemde *human in the loop* niet zonder meer voldoende bescherming biedt. Om daadwerkelijk betekenisvolle menselijke tussenkomst te waarborgen, moet de betrokken medewerker beschikken over voldoende informatie, tijd en autonomie om zelfstandig een besluit te nemen. In de praktijk is dit moeilijk te garanderen, mede omdat mensen geneigd zijn het besluit van het systeem te volgen ('computer says no').

AI-geletterdheid

Door het College voor de Rechten van de Mens werden zorgen geuit over de afzwakking van de verplichting voor alle AI-aanbieders en gebruiksverantwoordelijken om maatregelen te nemen die leiden tot een toereikend niveau van AI-geletterdheid bij hun personeel. Wil de AI-verordening effectief zijn, moet AI-geletterdheid wel op pijl zijn, zo meent het College. AI-geletterdheid is immers een noodzakelijke stap om in te kunnen schatten wanneer AI-inzet risico's voor grondrechten met zich meebrengt.

Registratie van hoog risico AI-systemen

Het College voor de Rechten van de Mens uitte voorts grote zorgen over het voorstel in de Omnibus AI om de registratieplicht te schrappen voor AI-systemen die geen hoog risico zouden zijn en uitsluitend worden ingezet voor beperkte of procedurele taken. De AI-verordening is in belangrijke mate gericht op hoog risico AI-systemen, juist omdat deze systemen gevolgen kunnen hebben voor de grondrechten van burgers. Een wijziging van de registratieplicht kan ertoe leiden dat systemen die feitelijk als hoog-risico moeten worden aangemerkt, niet als zodanig worden geregistreerd. Dit zou het toezicht op dergelijke systemen aanzienlijk bemoeilijken.

Bevoegdheidsvermindering grondrechtenautoriteiten

Een wijziging die mogelijk minder zichtbaar is dan andere onderdelen van de Omnibus AI maar in de praktijk verstrekende gevolgen kan hebben voor het toezicht, is de bevoegdheidsvermindering van grondrechtenautoriteiten. De AI-verordening kent grondrechtenautoriteiten de bevoegdheid toe om zelfstandig documentatie op te vragen bij organisaties die hoog risico AI-systemen gebruiken. Door de voorgestelde aanpassingen in de Omnibus AI zou deze bevoegdheid komen te vervallen. Volgens het College voor de Rechten van de Mens zou dit het voor grondrechtenautoriteiten in de Europese Unie aanzienlijk moeilijker maken om effectief toezicht te houden op de inzet van AI-systemen. In voorkomende gevallen zal eerst tussen de grondrechtenautoriteit en de markttoezichthouder moeten worden afgestemd of een verzoek om inzage in documentatie noodzakelijk is. Volgens het College leidt dit niet zozeer tot onduidelijkheid voor de onder toezicht staande organisatie, maar wel tot onzekerheid en praktische belemmeringen voor grondrechtenautoriteiten zelf.

Gespreksverslag nationale toezichthouders (AP en ACM)

Tijdens het gesprek met de Autoriteit Persoonsgegevens (AP) en de Autoriteit Consument & Markt (ACM) stonden vooral de gevolgen van de Omnibus AI en de Digitale Omnibus voor toezicht, privacy, uitvoerbaarheid en Europese samenwerking centraal.

De Omnibusprocedure

Beide toezichthouders hadden zorgen over de snelheid van de besluitvorming. De ACM gaf aan dat zij als toezichthouder geen partij is bij de onderhandelingen, maar merkte wel op dat meer tijd de zorgvuldigheid kan vergroten en dat een impact assessment behulpzaam is om de gevolgen van voorstellen goed te kunnen wegen.

De AP gaf aan dat omnibuswetgeving bedoeld is voor technische vereenvoudigingen, administratieve verlichting of verduidelijkingen, niet voor grote inhoudelijke wijzigingen die raken aan grondrechten. Volgens de AP gaan verschillende onderdelen van de voorstellen verder dan technische aanpassingen. Daarbij werd onder meer gewezen op wijzigingen rond de definitie van persoonsgegevens, de verwerking van bijzondere persoonsgegevens voor het trainen van AI en meldplichten bij datalekken.

Een impact assessment stelt de Europese wetgever en nationale parlementen in staat om de gevolgen van voorgestelde wetgeving zorgvuldig te wegen. Het Staff Working Document dat door de Europese Commissie is opgesteld, is volgens de AP te algemeen en oppervlakkig om als alternatief te kunnen gelden. Daarbij werd ook gewezen op het ontbreken van bredere betrokkenheid van maatschappelijke organisaties en andere stakeholders in de voorbereidende fase van de Omnibus AI en de Omnibus Digitaal.

Ook werd besproken dat de AI-verordening nog niet volledig is ingevoerd, terwijl er nu alweer wijzigingen worden voorgesteld. Volgens de AP kan dit leiden tot nieuwe rechtsonzekerheid en extra uitvoeringsproblemen. De AP geeft aanvullend aan dat

sommige voorgestelde wijzigingen juist nieuwe administratieve lasten en extra onduidelijkheid kunnen veroorzaken, omdat begrippen te breed of onduidelijk zijn geformuleerd.

Vereenvoudiging van digitale regelgeving

De ACM gaf aan dat vereenvoudiging van digitale regelgeving op zichzelf positief kan zijn. Volgens de ACM bestaat er op onderdelen overlap tussen verschillende verordeningen, definities, begrippen en verplichtingen. De ACM wees erop dat zij bevoegdheden heeft op grond van verschillende digitale wetten, waaronder de Digital Services Act, de Data Act, de Digital Markets Act en de platform-to-businessverordening. Omdat deze wetten elkaar op onderdelen raken, kan vereenvoudiging bijdragen aan meer duidelijkheid voor bedrijven, gebruikers en toezichthouders.

Volgens de ACM is effectieve Europese governance onontbeerlijk om digitale regelgeving goed te kunnen uitvoeren. Daarbij werd erop gewezen dat veel digitale regelgeving nog relatief nieuw is. De Dataverordening is bijvoorbeeld pas sinds september 2025 van toepassing. Toezichthouders zijn nog bezig met de inrichting van hun toezichtpraktijk en met de Europese samenwerking die daarvoor nodig is, terwijl de Dataverordening door de Omnibus Digitaal alweer wordt gewijzigd.

Het begrip 'persoonsgegevens' en privacy

De AP uitte zorgen over de voorgestelde wijziging van de definitie van persoonsgegevens. De AP merkte op dat de reikwijdte van het grondrecht op bescherming van persoonsgegevens in belangrijke mate afhangt van de definitie van persoonsgegevens. Wanneer die definitie wordt gewijzigd, wordt daarmee volgens de AP ook geraakt aan de reikwijdte van het grondrecht zelf.

De Europese Commissie verwijst bij deze wijzigingen naar recente jurisprudentie van het HvJEU, maar volgens de AP gaan de voorstellen verder dan een codificatie van die rechtspraak. Volgens de AP wordt in de voorstellen meer nadruk gelegd op een contextafhankelijke beoordeling van de vraag of gegevens als persoonsgegevens moeten worden aangemerkt. Dit kan problematisch zijn, omdat gegevens die op enig moment niet direct herleidbaar lijken tot een persoon, later door combinatie met andere gegevens, technologische ontwikkelingen of datalekken alsnog herleidbaar kunnen worden.

De AP gaf daarnaast aan dat een wijziging van de definitie ertoe kan leiden dat bepaalde gegevens waarmee burgers kunnen worden gevolgd, geanalyseerd of geprofileerd niet langer onder de bescherming van de AVG vallen. Dat kan de rechtsbescherming van burgers verminderen. Onduidelijkheid over de definitie van persoonsgegevens kan ook voor bedrijven problematisch zijn, omdat zij telkens opnieuw moeten bepalen wanneer gegevens wel of niet onder het regime van de AVG vallen.

Gebruik bijzondere persoonsgegevens voor trainen AI

Daarnaast wees de AP erop dat het expliciet noemen van “gerechtvaardigd belang” als grondslag voor AI-training volgens haar onnodig is, omdat die grondslag al bestaat. Een specifieke verwijzing naar de grondslag kan de indruk wekken dat grootschalige verwerking van persoonsgegevens in beginsel altijd op deze grondslag kan worden gebaseerd. Daarmee kan de drempel voor 'scraping' worden verlaagd, met name voor grote technologiebedrijven. Een bepaling die bedoeld is om te verduidelijken, roept hierdoor juist nieuwe rechtsonzekerheid op over wanneer gerechtvaardigd belang wel of niet is toegestaan als grondslag.

Transparantie en toezicht

De AP benadrukte dat transparantie- en verantwoordingsverplichtingen essentieel zijn voor effectief toezicht. Wanneer documentatieplichten, transparantieverplichtingen of verantwoordingsverplichtingen worden geschrapt of afgezwakt, krijgen toezichthouders minder grip om te beoordelen wat bedrijven en overheden doen. In dat licht werd stilgestaan bij meldingen van datalekken. De AP was kritisch op voorstellen om de drempel voor het melden van datalekken bij de toezichthouder te verhogen: organisaties moeten dan alleen nog melden als zij een hoog risico zien voor burgers. In de praktijk ziet de AP echter dat organisaties de risico's van een datalek vaak onderschatten. 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.

AI-geletterdheid

Volgens de AP wordt de verplichting rond AI-geletterdheid in de Omnibus AI te vrijblijvend gemaakt. Waar organisaties nu zelf verantwoordelijk zijn voor voldoende kennis en vaardigheden binnen hun organisatie, verschuift de nadruk in het voorstel naar het bevorderen of aanmoedigen van AI-geletterdheid door de Europese Commissie en de lidstaten. De AP acht dat onwenselijk, omdat AI-systemen steeds complexer en ingrijpender worden. Juist daarom zouden organisaties verplicht moeten worden om te investeren in kennis en training van medewerkers. Als AI-geletterdheid geen duidelijke verplichting meer is, wordt het bovendien moeilijker om toezicht te houden op de vraag of organisaties hun medewerkers voldoende toerusten voor verantwoord gebruik van AI.

De AP lichtte toe dat zij op dit moment al veel voorlichting geeft over AI-geletterdheid. Zodra de AP formele bevoegdheden heeft op grond van de nationale uitvoeringswet, wil zij organisaties kunnen vragen hoe zij invulling geven aan deze verplichting.

Platform-to-businessverordening

De ACM ging specifiek in op de platform-to-businessverordening. De verordening is volgens ACM bedoeld om zakelijke gebruikers van online platforms en zoekmachines, waaronder mkb-ondernemingen, meer transparantie en verhaalsmogelijkheden te bieden. Volgens de ACM heeft de verordening daarmee een eigen doelstelling, reikwijdte en beschermingsniveau en kan zij niet zonder meer worden vervangen door de Digital Services Act of de Digital Markets Act. De ACM benadrukte dat de verordening in de praktijk daadwerkelijk betekenis heeft. In Nederland zijn volgens de ACM tientallen tot mogelijk meer dan honderd signalen en meldingen ontvangen over de platform-to-businessverordening.

Nederland heeft in Europees verband aangegeven dat het verminderen van overlap wenselijk kan zijn, maar dat volledige intrekking van de P2B-verordening te ver gaat en de positie van mkb'ers kan verzwakken. De ACM gaf in het gesprek aan dat de Nederlandse argumenten op dit punt lijken te zijn gehoord en dat zij daarover enigszins gerustgesteld is.

Cloudregels

De ACM ging uitgebreid in op de cloud-bepalingen in de Data Act. Een belangrijk aandachtspunt betreft de uitzondering voor maatwerkdiensten. Volgens de ACM kunnen clouddaanbieders zich mogelijk vaker op maatwerkafspraken beroepen, omdat clouddiensten vaak zijn toegesneden op de wensen van een klant. Daardoor kan discussie ontstaan over de vraag of overstapverplichtingen wel of niet gelden. Dit kan vendor lock-in in stand houden of versterken. Ook langlopende contracten kunnen volgens de ACM problematisch zijn wanneer zij door overgangs- of uitzonderingsbepalingen buiten bepaalde verplichtingen vallen.

De ACM merkte op dat de Omnibus op dit punt haar doel voorbij kan schieten. Waar vereenvoudiging wordt beoogd, kunnen aanvullende uitzonderingen juist nieuwe complexiteit en uitvoeringsvragen oproepen.

Europese samenwerking en governance

De ACM benadrukte dat goede Europese samenwerking tussen toezichthouders noodzakelijk is. Veel digitale diensten worden namelijk aangeboden door ondernemingen die in meerdere lidstaten actief zijn. Dit vraagt om een zo uniform mogelijke uitleg en uitvoering van de regels. De ACM vindt het positief dat aandacht wordt besteed aan de European Innovation Data Board als coördinatiemechanisme. Wel wees de ACM erop dat bij toezicht op cloud- en datadiensten nog steeds een formeel samenwerkingsmechanisme tussen nationale toezichthouders en de Europese Commissie ontbreekt. De Omnibusvoorstellen lossen dit volgens de ACM niet op

De AP geeft aan dat in de Omnibus AI ook aandacht is voor het versterken van samenwerking tussen toezichthouders. De AP geeft hier op het gebied van de AI-verordening samen met de Rijksinspectie Digitale Infrastructuur (RDI) al vorm aan.

Gespreksverslag vertegenwoordigers bedrijfsleven (VNO-NCW en ATR)

Tijdens het gesprek met VNO-NCW en ATR stond de vraag centraal hoe de Omnibusvoorstellen tot stand zijn gekomen en wat de gevolgen daarvan zijn voor regeldruk en uitvoerbaarheid voor het bedrijfsleven.

De Omnibusprocedure

ATR plaatste vraagtekens bij de snelheid waarmee de Omnibusprocedure wordt doorlopen. ATR onderschrijft het belang van het verminderen van regeldruk, maar benadrukte dat bij een omvangrijk pakket met uiteenlopende wijzigingen een zorgvuldige afweging van de impact van alle onderdelen noodzakelijk is. Volgens ATR zou de Europese Commissie specifiekere moeten onderbouwen waarom sprake is van zodanige urgentie dat wijziging van het regelgevend kader via een Omnibusprocedure gerechtvaardigd is. ATR wees er daarnaast op dat veel Europese regelgeving in kort tijd wordt aangepast, terwijl deze regelgeving soms nog maar net is ingevoerd. Volgens ATR leidt dit tot onzekerheid en maakt dit het lastiger voor bedrijven om regelgeving te implementeren.

VNO-NCW merkte op dat bij de totstandkoming van reguliere Europese regelgeving meerdere impact assessments nodig zijn dan nu worden uitgevoerd (bijvoorbeeld een cumulatieve impact assessment van de samenhangende regels op het bedrijfsleven). Daarbij werd opgemerkt dat impact assessments niet alleen aan het begin van een wetgevingsproces van belang zijn, maar ook na substantiële wijzigingen in de triloofase. Volgens VNO-NCW heeft deze fase in de praktijk het karakter van een “black box”, omdat daarin doorgaans grote wijzigingen worden aangebracht zonder dat de gevolgen daarvan worden getoetst. De omnibussen - Omnibus AI en de Omnibus Digitaal - zijn bedoeld als technische aanpassingen om de coherentie tussen de verschillende regels te herstellen, meer duidelijkheid te scheppen en te zorgen voor meer proportionaliteit (codificaties van uitspraken van het Europese Hof van Justities, proportionaliteit brengen in meldingen, rapportage- en documentatieverplichtingen, e.d.).

ATR merkte op dat de Europese Commissie inmiddels heeft aangekondigd dat toekomstige omnibusvoorstellen vaker binnen de Better Regulation-principes zullen vallen en dat vaker impact assessments zullen worden uitgevoerd.

Volgens VNO-NCW zou de Europese Commissie voorafgaand aan nieuwe voorstellen nadrukkelijker moeten bezien hoe verschillende regelgevingskaders op elkaar

aansluiten. De huidige Omnibusvoorstellen werden in dat verband omschreven als herstelacties op wetgeving die eerder in afzonderlijke silo's tot stand is gekomen en daardoor onvoldoende samenhang vertoont. Voor het bedrijfsleven is het volgens VNO-NCW van groot belang dat meer coherentie tussen regels wordt aangebracht en dat meer aandacht uitgaat naar realistische implementatietermijnen.

Vermindering van regeldruk

De ATR constateerde dat er in de praktijk vaak een groot verschil zit tussen de door de Europese Commissie berekende regeldrukgevolgen en de omvang van die gevolgen in de praktijk. Europese kostencalculaties kunnen soms substantieel lager uitvallen dan de daadwerkelijke lasten. De ATR benadrukte ook dat de cumulatieve kosten van alle wet- en regelgeving op verschillende terreinen beter in beeld moet worden gebracht.

ATR benadrukte daarnaast dat regeldruk niet uitsluitend kwantitatief moet worden beoordeeld, maar ook in relatie tot begrijpelijkheid, uitvoerbaarheid en toezicht. Volgens ATR kan regelgeving op papier eenvoudiger lijken, terwijl de feitelijke toepassing voor bedrijven juist complexer wordt.

VNO-NCW onderschreef dit punt en benadrukte dat het ontbreken van voldoende inzicht in cumulatieve kosten voor het bedrijfsleven aanzienlijke problemen oplevert.

Impact wijzigingen aan de AVG voor bedrijfsleven

VNO-NCW steunt de voorgestelde gerichte aanpassingen van de AVG. Bedrijven hebben last van de verschillen in de uitleg van de AVG tussen de toezichthouders in de verschillende lidstaten. De voorgestelde wijzigingen worden door VNO-NCW slechts als 'babystapjes' gezien.

Toezicht

ATR wees erop dat toezicht ingewikkelder wordt wanneer regelgeving onduidelijk is of vaak wordt aangepast. Dit is voor kleine bedrijven niet te voorzien.

VNO-NCW gaf aan dat er inmiddels vaker overleg plaatsvindt met de Autoriteit Persoonsgegevens. Een meedenkende houding van toezichthouders is belangrijk voor goede en werkbare uitvoering van digitale regelgeving.