AH 2056

2026Z07492

Antwoord van staatssecretaris Aerdts (Economische Zaken en Klimaat) (ontvangen 28 mei 2026)

Zie ook Aanhangsel Handelingen, vergaderjaar 2025-2026, nr. 1722

1
Hoe beoordeelt u het besluit van het grootste Nederlandse pensioenfonds (ABP) om zich terug te trekken uit Palantir vanwege zorgen over mensenrechten en ethisch verantwoord investeren?

Antwoord
Een pensioenfondsbestuur is verantwoordelijk voor het beleggingsbeleid bij een pensioenfonds en ik geef daar geen oordeel over. Voor beleggingen zijn pensioenfondsen gehouden aan de *prudent person* regel. Deze regel stelt dat het vermogen in het belang van de deelnemers en pensioengerechtigden moet worden belegd. ABP weegt daarin tal van aspecten af, waaronder rendement, risico, kosten, ethische aspecten, mensenrechten en duurzaamheid. Deze afwegingen en de uiteindelijke investeringsbeslissingen die daaruit volgen zijn aan het ABP-bestuur.

2
Deelt u de zorg dat afhankelijkheid van buitenlandse technologiebedrijven zoals Palantir de digitale soevereiniteit van Nederland kan ondermijnen? Zo nee, waarom niet?

Antwoord
Het voorkomen en waar nodig mitigeren van risicovolle strategische afhankelijkheden in digitale technologie is een prioriteit van het kabinet. Daarbij wordt gekeken naar alle lagen van de digitale stack. Versterking van onze positie op AI heeft een centrale plek in verschillende beleidskaders, zoals de Agenda Digitale Open Strategische Autonomie en de Nationale Technologiestrategie. Hiertoe neemt het kabinet stimulerende maatregelen (*promote*), beschermende maatregelen (*protect*) en maatregelen tot het verdiepen van internationale samenwerking (*partnership*).

3
Kunt u uiteenzetten waar binnen de overheid de diensten en producten van Palantir worden gebruikt en waarvoor deze worden ingezet? Zo nee, waarom niet?

Antwoord
In antwoord op diverse Kamervragen van het lid Van Houwelingen (FvD),[1], evenals van de leden Van Vroonhoven en Six Dijkstra,[2] is aangegeven dat op dit moment alleen de politie en Defensie gebruik maken van Palantir.

De politie gebruikt de software van Palantir enkel binnen de zogenaamde «Raffinaderij». «De Raffinaderij» is een analyseomgeving waar Palantir onderdeel van uitmaakt. Deze wordt alleen aangewend voor de bestrijding van zware en georganiseerde criminaliteit

[1] Met als kenmerk 2025Z14552, 2025Z14549, 2025Z14551, 2025Z14550, 2025Z14548, 2025Z14553, 2025Z15452 en 2025Z19783.
[2] Met als kenmerk 2025Z15031.

en het voorkomen van aanslagen.

Binnen de Nederlandse krijgsmacht wordt gebruik gemaakt van de Palantir-software in het kader van interoperabiliteit tussen NAVO-partners ter ondersteuning van het militaire optreden.

4
Hoe beoordeelt u het gebruikmaken door Nederlandse (semi-)overheidsorganisaties van technologie van bedrijven zoals Palantir, waarover ernstige zorgen bestaan over betrokkenheid bij mensenrechtenschendingen? En op welke gronden wordt dit beoordeeld?

Het kabinet zal zich immer inzetten voor de bescherming van mensenrechten en de democratische rechtstaat, ook bij de inzet van technologie zoals AI. Daarbij heeft het kabinet ook aandacht voor de mogelijk discriminerende aspecten van technologie, en het beschermen van de democratie.

5
Welke ethische kaders hanteert het kabinet bij de inkoop en inzet van data-analyse- en AI-systemen van commerciële partijen zoals Palantir, en hoe worden deze kaders in de praktijk toegepast en gehandhaafd?

Antwoord
Vanuit de Nederlandse Digitaliseringsstrategie (NDS) werk ik aan een AI-inkoopaanpak. Hierin worden de inzichten uit de ethische kaders omtrent algoritmen en AI vanuit de overheid gebundeld, zoals het Algoritmekader en de leidraad van de Community of Practice Digitale Innovaties vanuit het Expertisecentrum Aanbesteden PIANOo. Daarin wordt bijvoorbeeld aangespoord een Fundamental Rights Impact Assessment (FRIA) uit te voeren, wat volgens de AI-verordening verplicht wordt bij hoog-risico AI-systemen. Een mogelijke invulling van zo'n FRIA is het Impact Assessment Mensenrechten en Algoritmes (IAMA). De uitkomsten van een IAMA kan leiden tot het treffen van maatregelen om mensenrechten te beschermen door de opdrachtgever of opdrachtnemer. In het Commissiedebat Digitaliserende overheid van 29 januari 2026 heeft de toenmalige staatssecretaris van Koninkrijksrelaties en Digitale Zaken toegezegd dat deze AI-inkoopaanpak in 2026 met uw Kamer zal worden gedeeld.

6
Welke concrete waarborgen, zoals toezicht, impact assessments en transparantiemechanismen, worden ingezet om te voorkomen dat het gebruik van dergelijke technologie leidt tot discriminatie, profilering of schending van privacyrechten?

Antwoord
Voorafgaand aan een voorgenomen gegevensverwerking, al dan niet door een leverancier van diensten, wordt een data protection impact assessment (DPIA) uitgevoerd om de risico's voor de rechten en vrijheden van betrokkenen in kaart te brengen. Beoordeeld wordt welke (aanvullende) maatregelen getroffen moeten worden om eventuele risico's voor de bescherming van persoonsgegevens en de rechten en vrijheden van betrokkenen zoveel mogelijk te mitigeren. In geval van doorgifte van persoonsgegevens aan landen buiten de EER wordt een data transfer impact assessment (DTIA) uitgevoerd, om te beoordelen of het betreffende land of internationale organisatie een passend beschermingsniveau waarborgt. Zoals eerder gemeld, wordt de FRIA volgens de AI-verordening verplicht bij hoog-risico AI-systemen. Een mogelijke

invulling van zo'n FRIA is het IAMA. Wat de verantwoorde en transparante inzet van algoritmen en AI binnen de overheid betreft, wordt daarnaast ook ingezet op instrumenten als het Algoritmeregister en het Algoritmekader. In mijn brief aan de Kamer van 20 april heb ik u tevens geïnformeerd over de wijze waarop het kabinet voornemens is het toezicht op de naleving van de Europese AI-verordening vorm te geven.[3]

Bij een verwerking van persoonsgegevens door een leverancier worden met deze leverancier afspraken gemaakt over de naleving van de mitigerende maatregelen. Deze maatregelen gelden voor de gehele toeleverancierskketen. De verwerkingsverantwoordelijke kan bij de leverancier informatie opvragen over de naleving van de betreffende maatregelen. Het uitvoeren van dergelijke assessments is een verantwoordelijkheid van de verwerkingsverantwoordelijke.

7
Bent u bereid om aanvullende richtlijnen of toetsingskaders te ontwikkelen voor samenwerking met technologiebedrijven die actief zijn in veiligheids- en surveillancedomeinen, die de digitale soevereiniteit ten goede komen? Zo nee, waarom niet?

Antwoord
In de NDS wordt onder de versneller versterking digitale weerbaarheid en digitale autonomie tevens gewerkt aan kaders die de digitale autonomie ten goede komen. Deze kaders worden sectorneutraal opgesteld, waardoor deze kaders naast het veiligheids- en surveillancedomein, ook in andere situaties gebruikt kunnen worden.

8
Bent u bereid om, in navolging van het besluit van ABP, voortaan expliciet en vooraf te toetsen of samenwerkingen met technologiebedrijven zoals Palantir verenigbaar zijn met Nederlandse en Europese normen, en deze toets openbaar te maken? Zo nee, waarom niet?

Antwoord
Zoals uit de voorgaande antwoorden ook blijkt zijn er diverse instrumenten, of worden deze op dit moment ontwikkeld, waarmee getoetst wordt of, op welke wijze en met welke eventuele aanvullende maatregelen bepaalde diensten verenigbaar zijn met Nederlandse en Europese normen. Het openbaar maken van dergelijke toetsen is aan de opdrachtgevende organisatie zelf, maar is niet wettelijk verplicht. Er kunnen moverende redenen zijn om dit ook niet te doen.

9
Zou u deze vragen afzonderlijk van elkaar kunnen beantwoorden?

Antwoord
Ja.

[3] Kamerstukken II 2025-26, 22 112, nr. 4318