

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

2877

Vragen van het lid **Van Houwelingen** (FvD) aan de Minister van Justitie en Veiligheid over *Palantir* (ingezonden 11 juli 2025).

Antwoord van Minister **Van Weel** (Justitie en Veiligheid) (ontvangen 20 augustus 2025) Zie ook Aanhangsel Handelingen, vergaderjaar 2024–2025, nr. 2790

Vraag 1

Welke organisatieonderdelen binnen uw ministerie maken/maakten gebruik van of hebben/hadden toegang tot de Palantir software?¹

Antwoord 1

Palantir is een technologiebedrijf dat gespecialiseerd is in software voor databeheer en -analyse. Organisaties maken onder andere van Palantir software gebruik om grote hoeveelheden data vanuit verschillende databronnen met elkaar te integreren. Deze data-integratie leidt tot inzicht/overzicht, waarmee complexe vraagstukken kunnen worden behandeld. 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 en het voorkomen van aanslagen. Over het (kortstondige) gebruik van Palantir software door de zes zuidelijke Veiligheidsregio's ten behoeve van informatiegestuurde veiligheid is uw Kamer op 21 juni 2021 geïnformeerd.² Dit gebruik is reeds in 2021 beëindigd en was op geen enkele wijze gelieerd aan de analyseomgeving «de Raffinaderij». Alleen openbare en publiek toegankelijke data zijn door zes Veiligheidsregio's gebruikt. Palantir had geen toegang tot data van de veiligheidsregio's. In het Nieuw Rechts artikel «*Hoe de Nederlandse overheid stilletjes een politiestaat optuigt met Palantir*» van 10 juli 2025 wordt geschreven dat NCTV nauw samenwerkt met Palantir. Er is in het heden of verleden geen actief gebruik van Palantir (licenties) bij het organisatieonderdeel NCTV. Uit de uitgevoerde inventarisatie naar Palantir software gebruik binnen mijn ministerie is tot op heden geen andere aanwending van deze software gebleken.

¹ Nieuw Rechts, 10 juli 2025, Hoe de Nederlandse overheid stilletjes een politiestaat optuigt met Palantir (<https://nieuwrechts.nl/105250-hoe-de-nederlandse-overheid-stilletjes-een-politiestaat-optuigt-met-palantir>).

² Kamerstukken II, 2020–2021, nr. 3011

Vraag 2

Zijn er buiten de «Raffinaderij» nog andere projecten of initiatieven (geweest) die gebruik maken/maakten van Palantir software? Zo ja, welk organisatieonderdeel ontplooit/ontplooidde dat initiatief en onder welke projectnaam of titel?

Antwoord 2

Nee, zie voor een uitgebreide toelichting de beantwoording van de eerste vraag.

Vraag 3

Welke organisatieonderdelen (waaronder ook samenwerkingsverbanden als de Regionale Informatie- en Expertisecentra (RIEC's), Landelijk Informatie- en Expertisecentrum (LIEC), infobox Crimineel en Onverklaarbaar Vermogen (iCOV), etc.) en /of functionarissen maken/maakten gebruik van of hebben/hadden toegang tot de informatieproducten uit de «Raffinaderij» en / of Palantir software?

Antwoord 3

Behoudens de politie en de zes veiligheidsregio's³ in het verleden maken organisatieonderdelen van het Ministerie van Justitie & Veiligheid en/of aan Justitie & Veiligheid gelieerde samenwerkingsverbanden (waaronder de Regionale Informatie- en Expertisecentra, het Landelijk Informatie- en Expertisecentrum, en de infobox Crimineel en Onverklaarbaar Vermogen) geen gebruik van Palantir software. Alleen de politie maakt gebruik van de analyseomgeving «de Raffinaderij». Geen andere organisatieonderdelen van het Ministerie van Justitie & Veiligheid dan de politie en geen andere functionarissen dan de politiefunctionarissen hebben nu en/of hadden in het verleden toegang tot de analyseomgeving «de Raffinaderij». Informatieproducten afkomstig uit de analyseomgeving «de Raffinaderij» worden niet gedeeld met partijen buiten de politie. Wel kan het zijn als op basis van een signaal afkomstig uit een informatieproduct vanuit de analyseomgeving «de Raffinaderij» sprake blijkt van hetzij een concrete verdenking van zware en georganiseerde criminaliteit dan wel een hoge kans op aanslagen dat de politie op basis van dit signaal op casuïstiek niveau contact legt met haar ketenpartners.

Vraag 4

Zijn er organisatieonderdelen die onder uw ministeriële verantwoordelijkheid vallen die data delen met de «Raffinaderij» of andere Palantir-gerelateerde initiatieven, en zo ja, welke organisatieonderdelen zijn dat?

Antwoord 4

De politie ontvangt of ontving ten aanzien van de analyseomgeving «de Raffinaderij» geen data van andere organisatieonderdelen. Vice versa hebben en/of hadden geen andere organisatieonderdelen of functionarissen dan de politie toegang tot de analyseomgeving «de Raffinaderij» of hebben nu en/of hadden die in het verleden toegang tot de informatieproducten uit deze analyseomgeving. Onder de verantwoordelijkheid van de Minister van Justitie en Veiligheid vallen geen andere organisatieonderdelen die andere Palantir-gerelateerde initiatieven hebben of hadden lopen.

Vraag 5

Uit vrijgegeven Wet open overheid (Woo)-documenten blijkt dat de verwerving van de Palantir software heimelijk heeft plaatsgevonden; klopt het dat hierdoor regels voor een openbare aanbesteding niet zijn gevolgd?

Antwoord 5

De heimelijke verwerving heeft in 2018 plaatsgevonden met een beroep op art. 2.23, lid 1 sub e van de AW 2012. Deze bepaling stelt dat de aanbestedingsregels niet van toepassing zijn op overheidsopdrachten voor leveringen, diensten of werken die geheim zijn verklaard, of waarvan de uitvoering met

³ De Veiligheidsregio's zijn overigens geen departementsonderdeel.

bijzondere veiligheidsmaatregelen gepaard moet gaan, of indien bescherming van wezenlijke belangen van Nederland dit vereist. Zie voorts beantwoording van vraag 6.

Vraag 6

Wat waren de redenen voor het heimelijk verwerven van de Palantir software?

Antwoord 6

De redenen voor het heimelijk verwerven waren:

- a. De thema's waarop de analyseomgeving «de Raffinaderij» en daarmee Palantir wordt ingezet zijn zeer gevoelig en kennen een hoog afbreukrisico (bestrijding van zware en georganiseerde criminaliteit en het voorkomen van aanslagen).
- b. Openbaarheid van gebruikte methoden, eventuele tijdlijnen en systeem-informatie levert mogelijk een afbreukrisico op voor de betreffende onderzoeken in de analyseomgeving «de Raffinaderij».
- c. Een deel van de software is zelf ontwikkeld door een team van de politie dat zeer nauw betrokken is bij de operatie. Openbaarmaking zou inzicht geven in gehanteerde onderzoeksmethoden.
- d. De genoemde risico's kunnen niet afdoende worden beperkt met minder ingrijpende maatregelen. Immers, ook bij het toepassen van de (Europese) niet-openbare procedure zal gevoelige/specifieke informatie moeten worden gedeeld met een grote kring van gegadigden. Zelfs indien ondernemingen vooraf zouden worden gescreeend en worden verplicht tot geheimhouding, leidt een dergelijke aanbesteding tot kennis van specificaties bij een te grote groep.

Vraag 7

Kunnen de vragen afzonderlijk en binnen drie weken worden beantwoord?

Antwoord 7

De vragen zijn zo snel mogelijk beantwoord.