Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

> Retouradres Postbus 20011 2500 EA Den Haag

Aan de voorzitter van de Tweede Kamer der Staten-Generaal
Postbus 20018
2500 EA Den Haag

DG Digitalisering & Overheidsorganisatie
DGDOO-CIO-Inform.beveiliging & Privacy

Turfmarkt 147
2511 DP Den Haag
Postbus 20011
2500 EA Den Haag

Onze referentie
2026-0000142728

Datum 13 april 2026
Betreft Beantwoording Kamervragen over dat de NS ICT uitbesteedt aan een Amerikaanse leverancier

Hierbij bied ik u, mede namens de staatssecretaris van Infrastructuur en Waterstaat, de antwoorden aan op de schriftelijke vragen die zijn gesteld door de leden Kathmann en De Hoop (beiden GroenLinks-PvdA) over dat de NS ICT uitbesteedt aan een Amerikaanse leverancier. Deze vragen werden ingezonden op 11 februari 2026, met kenmerk 2026Z02956.

De staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,

Eric van der Burg

DG Digitalisering & Overheidsorganisatie
DGDOO-CIO-Inform.beveiliging & Privacy

Onze referentie
2026-0000142728

Vragen van de leden Kathmann en De Hoop (beiden GroenLinks-PvdA) aan de Staatssecretarissen van Binnenlandse Zaken en Koninkrijksrelaties en van Infrastructuur en Waterstaat over het bericht dat de NS ICT uitbesteedt aan een Amerikaanse leverancier (ingezonden 11 februari 2026).

Vraag 1
Bent u bekend met het bericht «NS besteedt ict deels uit aan Amerikaanse leverancier»?1
Ja.

Vraag 2
Kunt u toelichten welke ICT-processen van de NS precies worden uitbesteed?2 Zijn dit (onderdelen van) kritieke processen met gevolgen voor de continuïteit van de NS indien ze langer dan één dag uitvallen?
De aanbesteding betreft een aantal verschillende systemen. Het gaat om:

- Systemen die gebruikt worden in de werkplaatsen, zoals bijvoorbeeld systemen die roostering van monteurs regelen.
- Systemen die de bedrijfsvoering ondersteunen. Het gaat dan bijvoorbeeld om de uitgifte van toegangspassen voor bedrijfspanden, de beheeromgeving van kassasystemen en prikklokken voor retailmedewerkers op stations en het systeem voor de financiële planning van de financiële afdeling, het afhandelingssysteem voor boetes aan reizigers, de aansturing van systemen voor camera's en meldkamer ter ondersteuning van de medewerkers Veiligheid en Service, het beheer van de alarmzuilen op stations en het controlesysteem van de verwerking van de OV-chipkaart-transacties (dit zijn de technische sleutels van de in- en uitchecks, zonder de bijbehorende persoonsgegevens).

Uitval van deze systemen heeft niet direct gevolgen voor het rijden van treinen. Wel kan de uitval gevolgen hebben voor andere aspecten van de dienstverlening, wat uiteindelijk tot hinder voor reizigers kan leiden. Het is overigens goed om te beseffen dat bovenstaande functies die onderdeel zijn van de uitbesteding, nu ook al zijn ondergebracht bij derde partijen.

Vraag 3
Klopt het dat er ook (onderdelen van) beveiligingssystemen worden uitbesteed aan een Amerikaans bedrijf? Welke gevolgen heeft dit voor de digitale autonomie van de Nederlandse (spoor)infrastructuur?
Zie voor een opsomming van de betreffende systemen het antwoord op vraag 2. Het Security Operations Center wordt door NS zelf verzorgd, op dit moment in samenwerking met een Nederlands IT-bedrijf. In deze aanbesteding heeft NS de cyberrisico's in kaart gebracht en in lijn daarmee passende eisen gesteld en een passend risicomanagementsysteem gekozen.

DG Digitalisering & Overheidsorganisatie
DGDOO-CIO-Inform.beveiliging & Privacy

Onze referentie
2026-0000142728

Vraag 4
Deelt u de opvatting van de NS dat de uitbestede processen niet missiekritisch zijn? Kunt u schetsen welke gevolgen het heeft voor de dienstverlening van de NS indien deze systemen wél uitvallen? Kunt u uitsluiten dat de uitvoering van de dienstverlening van NS (het laten rijden van treinen op het hoofdrailnet) in gevaar zou kunnen komen wanneer de betreffende systemen uitvallen? Zo ja, kunt u dit motiveren? Zo nee, deelt u dan de zorgen over deze uitbesteding?

Zie ook het antwoorden op vragen 2 en 3. Uitval van deze systemen heeft geen of beperkte directe gevolgen voor het rijden van treinen. Wel kan de uitval gevolgen hebben voor andere aspecten van de dienstverlening. De daadwerkelijke impact hangt af van de aard en de duur van de onderbreking en het specifieke onderdeel van de dienstverlening dat geraakt wordt.
Hierbij dient te worden benadrukt dat de grootste bedreiging voor de continuïteit van de (digitale) dienstverlening externe kwaadwillenden zijn. Hiertoe is het van belang dat de digitale diensten die worden afgenomen voldoen aan het vereiste beveiligingsniveau. De gekozen dienstverlener voldoet hieraan.

Vraag 5
Kan de Amerikaanse overheid, via wet- en regelgeving zoals de CLOUD Act, Foreign Intelligence Surveillance Act (FISA), en Executive Order 12333, toegang krijgen tot gevoelige gegevens over de Nederlandse spoorinfrastructuur? Kunt u dit met een ja of nee beantwoorden en dit met concrete verwijzing naar relevante juridische bronnen toelichten?

Diverse landen kennen inderdaad wet- en regelgeving met extraterritoriale werking die medewerking van dienstverleners bij gegevensverzoeken van veiligheidsdiensten verplicht, zoals de CLOUD Act, Executive Order 12333, en FISA sectie 702 in de VS. Voor EO12333 is geen medewerking van de leverancier vereist. Dergelijke wet- en regelgeving kan in bepaalde gevallen mogelijk leiden tot ongewenste toegang tot Nederlandse gegevens. Op basis van dergelijke regelgeving kan een onder Amerikaanse zeggenschap vallende organisatie de opdracht krijgen gegevens te verstrekken aan de Amerikaanse overheid. Zie verder het antwoord op vragen 2 en 3.

Vraag 6
Biedt de groeiende afhankelijkheid van Amerikaanse ICT-bedrijven de mogelijkheid voor de Verenigde Staten om druk uit te oefenen op Nederland, bijvoorbeeld door de continuïteit van de dienstverlening van de NS in gevaar te brengen?

In deze NS-casus ziet het kabinet geen aanleiding om aan te nemen dat door de inkoop van deze ICT-diensten de continuïteit van de dienstverlening in gevaar wordt gebracht of dat het gebruik van deze specifieke digitale dienst gebruikt zal worden om druk uit te oefenen op Nederland. Nederland en Europa zijn voor cruciale digitale infrastructuur sterk afhankelijk geworden van een klein aantal niet-Europese spelers. Dat maakt ons kwetsbaar in een wereld waarin technologie steeds vaker als geopolitiek machtsmiddel wordt ingezet. Dit levert efficiëntie en

toegang tot belangrijke functionaliteiten op, maar legt ook een kwetsbaarheid bloot ten aanzien van afhankelijkheid en digitale autonomie. Daarom is in algemene zin de inzet van het kabinet er op gericht om risicovolle strategische afhankelijkheden van derde landen af te bouwen en zoveel mogelijk te diversifiëren, ook op digitaal vlak.

Vraag 7
Deelt u de mening dat de NS digitale autonomie zou moeten betrachten en af zou moeten zien van deze aanbesteding bij een Amerikaans bedrijf? Welke concrete mogelijkheden ziet u hiertoe?

Zie het antwoord op vraag 8.

Vraag 8
Waarom voldeed KPN niet meer als aangewezen ICT-leverancier voor deze diensten? Was het strikt noodzakelijk om de ICT uit te besteden, en zo ja, waarom aan een niet-Europees bedrijf?

NS dient zicht te houden aan de Aanbestedingswet. Het eerdere contract met KPN liep af en kende ook geen verlengingsmogelijkheden meer. NS is dan verplicht de opdracht via een Europese Aanbestedingsprocedure in de markt te zetten. Daarbij stelt NS zeer uitgebreide eisen en criteria op het gebied van prijs, kwaliteit, beschikbaarheid (zo min mogelijk storingen) en cyberveiligheid. De Nederlandse dochter van een Amerikaanse onderneming kwam als beste uit de bus.

Vraag 9
Past de keuze van de NS om haar ICT uit te besteden aan een Amerikaans bedrijf binnen de ambitie van het kabinet om meer digitaal onafhankelijk te worden? Welke rol heeft de Staat als enig aandeelhouder hierin?

De gunning is een uitkomst van het verplichte Europese aanbestedingsproces. Het kabinet heeft als doel om bij digitale inkoop en aanbestedingen te gaan standaardiseren en centraliseren, waarbij onder meer gestuurd wordt op waarden zoals security-by-design, zero-trust, soevereiniteit, open source en ketenveiligheid.
Als aandeelhouder van NS staat de minister van Financiën op dit onderwerp meer op afstand: operationele zaken zoals de wijze van aanbesteden zijn primair de verantwoordelijkheid van het bestuur van de deelnemingen.

Vraag 10
Hoe kijkt u aan tegen de keuze van de NS om, tegen de achtergrond van de huidige geopolitieke situatie en nadat de Rijksoverheid herhaaldelijk het belang van digitale autonomie benadrukte, alsnog ICT uit te besteden aan een niet-Europees bedrijf?

Ik verwijs graag naar mijn antwoord op vraag 6, 8 en 9.

DG Digitalisering & Overheidsorganisatie
DGDOO-CIO-Inform.beveiliging & Privacy

Onze referentie
2026-0000142728

Vraag 11
Acht u de lange doorlooptijd van het contract, namelijk zes tot twaalf jaar, geschikt gezien de onzekerheid van de geopolitieke relatie met de Verenigde Staten?

Een dergelijke doorlooptijd is niet ongewoon gezien de implementatietijd en -kosten van een dergelijke migratie.

Vraag 12
Klopt het dat er geen nationale richtlijnen bestaan om Amerikaanse partijen te weren? Staat dit wel voorzien in het nieuwe cloudbeleid dat nog steeds in ontwikkeling is?

Het klopt dat er geen nationale richtlijnen zijn om Amerikaanse partijen te weren en de inzet van het kabinet is daar ook niet op gericht. Het Rijksbreed cloudbeleid is niet van toepassing op staatsdeelnemingen, en is landenneutraal opgesteld. Het kabinet heeft wel als doel om bij digitale inkoop en aanbestedingen te gaan standaardiseren en centraliseren, waarbij onder meer gestuurd wordt op waarden zoals security-by-design, zero-trust, soevereiniteit, open source en ketenveiligheid.

Vraag 13
Is in deze aanbesteding voldaan aan de Algemene Beveiligingseisen voor Rijksoverheidsopdrachten (ABRO), waarin staat dat er strenge eisen gesteld moeten worden aan digitale autonomie en soevereiniteit?

Het kabinet heeft besloten dat de departementen, hun diensten en agentschappen, en de politie vanaf 1 januari 2026 de ABRO gaan toepassen bij contracten met bedrijven als daarbij risico's voor de nationale veiligheid aanwezig zijn. De NS is geen onderdeel van deze organisaties. Voor de implementatie hiervan hebben deze inkopende organisaties tot eind 2027 de tijd gekregen. Daarover is uw Kamer geïnformeerd (TK 2025/2026 26643-1438). Als een inkopende organisatie, voordat zij besluit de ABRO toe te gaan passen, al een aanbestedingsproject in gang heeft gezet, is uitgangspunt dat deze aanbesteding niet alsnog onder de ABRO kan worden gebracht.

In bedoelde Kamerbrief is ook gemeld dat voorbereidingen worden getroffen om deze beveiligingseisen ook te laten toepassen door andere inkopende organisaties. Dat gaat om onder meer Zelfstandige Bestuursorganen, provincies, gemeenten, waterschappen en vitale sectoren. Momenteel wordt binnen het rijksbrede programma 'Veilig inkopen' onderzocht welke risico's deze organisaties lopen voor de nationale veiligheid. Het staat nog niet vast welke specifieke organisaties in dit onderzoek worden meegenomen. Voor deze inkopende organisaties worden de benodigde juridische instrumenten, financiën en organisatorische afspraken voorbereid. In het 3e kwartaal van 2026 wordt de Tweede Kamer over de stand van zaken van het programma 'Veilig inkopen' geïnformeerd.

De ABRO maakt onderdeel uit van een keten. De inkopende organisatie deelt bij aanvang van een aanbesteding mee dat de ABRO wordt toegepast. Als bij een

inkoop de Aanbestedingswet op Defensie- en Veiligheidsgebied (ADV) wordt gevolgd, dan biedt dat de mogelijkheid om alleen bedrijven uit de Europese Economische Ruimte én bedrijven uit nader te bepalen landen toe te laten als inschrijver op zo'n inkoop.

De ABRO ziet niet direct op digitale soevereiniteit en biedt geen directe mogelijkheden om ongewenste overnames te voorkomen of bepaalde aanbieders op voorhand uit te sluiten in een aanbesteding. Het Nationaal Bureau Industrieveiligheid (NBIV) controleert het bedrijf dat als winnaar uit zo'n aanbesteding komt of het aan de ABRO-eisen voldoet. Daarbij dient onder meer inzicht te worden gegeven in de organisatiestructuur van en de zeggenschap over een bedrijf. Als de risico's voor de nationale veiligheid niet kunnen worden beperkt, geeft NBIV geen ABRO-verklaring af en kan in beginsel geen contract worden afgesloten.

Bij een contract waarop de ABRO is toegepast, is de contractspartij verplicht om NBIV tijdig te informeren bij potentiële overnames of wisselingen in significante invloed. Het biedt opdrachtgever en NBIV daarmee de mogelijkheid om de risico's voor de nationale veiligheid te beperken. Indien die risico's niet kunnen worden beperkt, kan de ABRO-verklaring worden ingetrokken en kan de inkopende organisatie het contract ontbinden.

Vraag 14
Is het mogelijk om via het Cloud Sovereignty Framework van de EU wél voorkeur te geven aan Europese partijen bij ICT-aanbestedingen? Waarom is daar in dit geval geen gebruik van gemaakt?

Het Cloud Sovereignty Framework van de EU is niet van toepassing op deze tender en bestond nog niet ten tijde van het uitzetten van de onderhavige aanbesteding. Het is op basis van de aanbestedingsregels niet toegestaan om gedurende de aanbestedingsprocedure aanvullende eisen (zoals het EU Cloud Sovereignty Framework) toe te voegen.

Het Cloud Sovereignty Framework van de EU biedt kwalitatieve scoringseisen voor aanbestedende partijen en heeft als doel om een level playing field te bieden aan clouddienstverleners, en tevens om de sector richting Europese standaarden en waarden te drijven. Het Cloud Sovereignty Framework is dus niet gericht op het uitsluiten van partijen.

Vraag 15
Kunt u deze vragen afzonderlijk van elkaar en zo spoedig mogelijk beantwoorden, nog voordat er onomkeerbare stappen worden gezet?

De vragen zijn zo spoedig mogelijk beantwoord.