2026Z12034

(ingezonden 4 juni 2026)

Vragen van het lid Van den Berg (JA21) aan de staatssecretarissen van Binnenlandse Zaken en Koninkrijksrelaties en van Economische Zaken en Klimaat en de ministers van Binnenlandse Zaken en Koninkrijksrelaties en van Justitie en Veiligheid over digitale soevereiniteit, kritieke digitale overheidsinfrastructuur en de afhankelijkheden rond DigiD, Solvinity en Kyndryl.

Kunt u toelichten waarom de voor DigiD benodigde digitale infrastructuur en diensten niet rijksbreed zijn georganiseerd, maar via afzonderlijke aanbestedingen en contracten worden ingekocht? Welke afwegingen liggen hieraan ten grondslag?

Wanneer gaat het kabinet kritieke digitale overheidsvoorzieningen, zoals DigiD, MijnOverheid, Digipoort en vergelijkbare voorzieningen, wél rijksbreed organiseren of ten minste rijksbreed normeren?

Hoe en wanneer geeft het kabinet uitvoering aan de aangenomen motie-Van den Berg c.s. over een rijksbreed dataclassificatie- en datalocatiebeleid (Kamerstuk 26 643, nr. 1482)?

Welke concrete stappen zijn sinds aanneming van deze motie gezet, welke bewindspersoon is eerstverantwoordelijk en wanneer ontvangt de Kamer een voortgangsrapportage?

Welke voorzieningen kwalificeert het kabinet, naast DigiD, als kritieke digitale overheidsinfrastructuur?

Bestaat er inmiddels een rijksbreed overzicht van kritieke digitale overheidsvoorzieningen en de daarbij betrokken niet-Nederlandse of niet-Europese leveranciers? Zo nee, waarom niet?

Wanneer komt er een dergelijk overzicht, inclusief inzicht in cloud, hosting, beheer, datatoegang, encryptiesleutels, operationele zeggenschap, onderaannemers, ketenafhankelijkheden en exittermijnen?

Wat is het doel van het kabinet ten aanzien van de toekomstige inrichting van DigiD? Is het streven gericht op andere technologie, een andere leverancier, Europese of Nederlandse zeggenschap, publiek beheer of een combinatie daarvan?

Welke rol speelt digitale soevereiniteit precies bij de toekomstige inrichting van DigiD? Welke concrete risico’s worden hiermee beoogd te verminderen?

Hoe verhoudt het Nederlandse beleid zich tot landen die eveneens streven naar digitale autonomie, maar daarbij gebruikmaken van technologie van niet-Europese aanbieders?

In de kabinetsreactie van 23 mei 2025 op de motie-Koekkoek (Kamerstuk 26643, nr. 1338) werd gesteld dat er kwalitatief hoogwaardige Europese clouddiensten beschikbaar zijn. Op welke concrete marktverkenning, technische toets of aanbestedingservaring was die conclusie

gebaseerd? Zag die conclusie bovendien op generieke clouddiensten, of ook op kritieke digitale identiteitsinfrastructuur zoals DigiD, MijnOverheid en Digipoort?

Welke concrete stappen zijn tussen 23 mei 2025 en 2 juni 2026 gezet om Nederlandse of Europese alternatieven daadwerkelijk geschikt te maken voor het beheer van DigiD of vergelijkbare kritieke voorzieningen?

In eerdere beantwoording heeft u gesteld dat sprake is van gelijkwaardige technologieën van Europese en Nederlandse aanbieders. Wat verstaat het kabinet precies onder een “gelijkwaardig alternatief” voor de huidige DigiD-dienstverlening?

Welke criteria worden gehanteerd om vast te stellen of een alternatief gelijkwaardig is? Wordt daarbij gekeken naar functionaliteit, schaalbaarheid, beveiliging, beschikbaarheid, betrouwbaarheid, certificeringen, prestaties, migratierisico’s, operationele ervaring, continuïteit en bewezen beheer van kritieke digitale infrastructuur op nationale schaal?

Deelt u de opvatting dat DigiD vanwege zijn unieke en kritieke rol moeilijk één-op-één vergelijkbaar is met generieke cloud-, hosting- of authenticatiediensten? Zo nee, waarom niet? Zo ja, kunt u toelichten hoe deze unieke rol van DigiD zich verhoudt tot de conclusie van de ACM dat er voldoende concurrentie overblijft omdat er andere IT-dienstverleners zijn die soortgelijke diensten leveren?

Wat verstaat het kabinet in dit verband onder “soortgelijke diensten”? Gaat het daarbij om algemene IT-dienstverlening, of specifiek om bewezen beheer van kritieke digitale identiteitsinfrastructuur op nationale schaal?

Welke minimale eisen gelden voor cloud, hosting, beheer, encryptiesleutels, toegangsbeheer, logging, monitoring, incidentrespons, onderaannemers en operationele zeggenschap bij DigiD?

Hoe wordt geborgd dat encryptiesleutels, beheerrechten en operationele toegang tot DigiD niet onder zeggenschap vallen van niet-Europese moederbedrijven of buitenlandse wettelijke bevoegdheden?

Heeft iedere kritieke digitale overheidsvoorziening een actueel exitplan? Zo ja, hoe vaak worden deze exitplannen getest?

Welke kritieke digitale voorzieningen hebben een verwachte migratietermijn van meer dan zes maanden, en welke continuïteitsrisico’s levert dat op?

Welke onderdelen van de TFEV- of BTI-analyse rond Solvinity/Kyndryl kunnen openbaar met de Kamer worden gedeeld, en welke onderdelen kunnen vertrouwelijk worden verstrekt?

Kunt u de vragen afzonderlijk en voor het commissiedebat inzake Bescherming persoonsgegevens en grote datalekken van 25 juni aanstaande beantwoorden?